



Which CLI command is used to simulate traffic going through the firewall and determine which Security policy rule, NAT translation, static route, or PBF rule will be triggered by the traffic?

- A. check
- B. find
- C. test
- D. sim

Correct Answer: C

Reference:

<http://www.shanekillen.com/2014/02/palo-alto-useful-cli-commands.html>

— **xykusonu** Highly Voted 6 days, 19 hours ago

Answer (C) is the right . Ty (Exam For Sure)
upvoted 20 times

— **sov4** Highly Voted 1 year, 1 month ago

Hey everyone, it's July 31st 2023 and I just passed the exam today. Every single one of the questions, except for one, was in this dump. As of this post there are 554 questions in this dump. The newer ones regarding v10 and v11 are at the end; however, I had questions from all over this dump. If you study this dump end to end you'll do fine, at least at the time of this writing.

Most of the answers are wrong in here. Some of the answers provided by others are wrong as well. You need to do your own research. It will make you learn the material (which will help with questions not in this dump), and help remember the questions/answers when they come up.

Best of luck everyone. See you all back when it's time to recertify :-P
upvoted 19 times

— **ax_Network** Most Recent 1 month, 1 week ago

Selected Answer: C

C is Correct Answer
upvoted 1 times

— **arismendy** 1 month, 1 week ago

Hello Guys, I just pass the exam today Jul 22 2024, almost all the questions are in this dumb (I got 75 questions in the exam and almost 60 where from here and the other ones are related to other questions from here), I studied from CBT, Youtube videos and from the official study guide.

The new questions that i got where questions related to decryption, HA and zone protection. Like SOV4 said: "Most of the answers are wrong in here. Some of the answers provided by others are wrong as well. You need to do your own research".

I'm not from a English speaking country and i got some extra time for the exam and that helps me, just remember to keep an eye on the time.

Best of luck !
upvoted 3 times

— **CISCO101** 2 weeks, 4 days ago

How many percentage of wrong answer from 606 questions? Do you think it can be around 30% from 606 questions?
upvoted 1 times

— **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: C

C - Test

> test security-policy-match source <source IP> destination <destination IP/netmask> protocol <protocol number>
upvoted 1 times

— **Sammy3637** 9 months ago

Old question
upvoted 1 times

— **techplus** 11 months, 2 weeks ago

test nat-policy-match
upvoted 3 times

testman99 1 year, 6 months ago

not on exam, these are very old questions and answers. Everything is now PANOS11 and Panorama
upvoted 1 times

network_geek_2020 1 year, 6 months ago

C is correct
upvoted 1 times

Dilton 1 year, 7 months ago

I would like to know if recently someone have taken the exam and how much the percent of questions from this dump? Thanks in advance
upvoted 2 times

lol12 1 year, 10 months ago

Selected Answer: C

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIQSCA0>
upvoted 1 times

TAKUM1y 1 year, 11 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-cli-quick-start/use-the-cli/test-the-configuration/test-policy-matches>
upvoted 1 times

GheeHong 2 years, 1 month ago

Failed Exam at 2 weeks ago (13 July) . Only had about 8 questions from this dump.
More questions focus on PAN-OS 10.1. Appreciate examtopic able to update PCNSE dump questions, please.
upvoted 4 times

bimyo 2 years, 1 month ago

Indeed a new exam, with only around 25% from this dump. So the updated questions would be needed.
upvoted 3 times

IckoPCNSE 2 years, 1 month ago

There is a completely new exam. Not more than 10 questions are from here. I failed about a month ago and you definitely have to update the questions please, please, please ! :)
upvoted 2 times

Meko 2 years, 2 months ago

Selected Answer: C

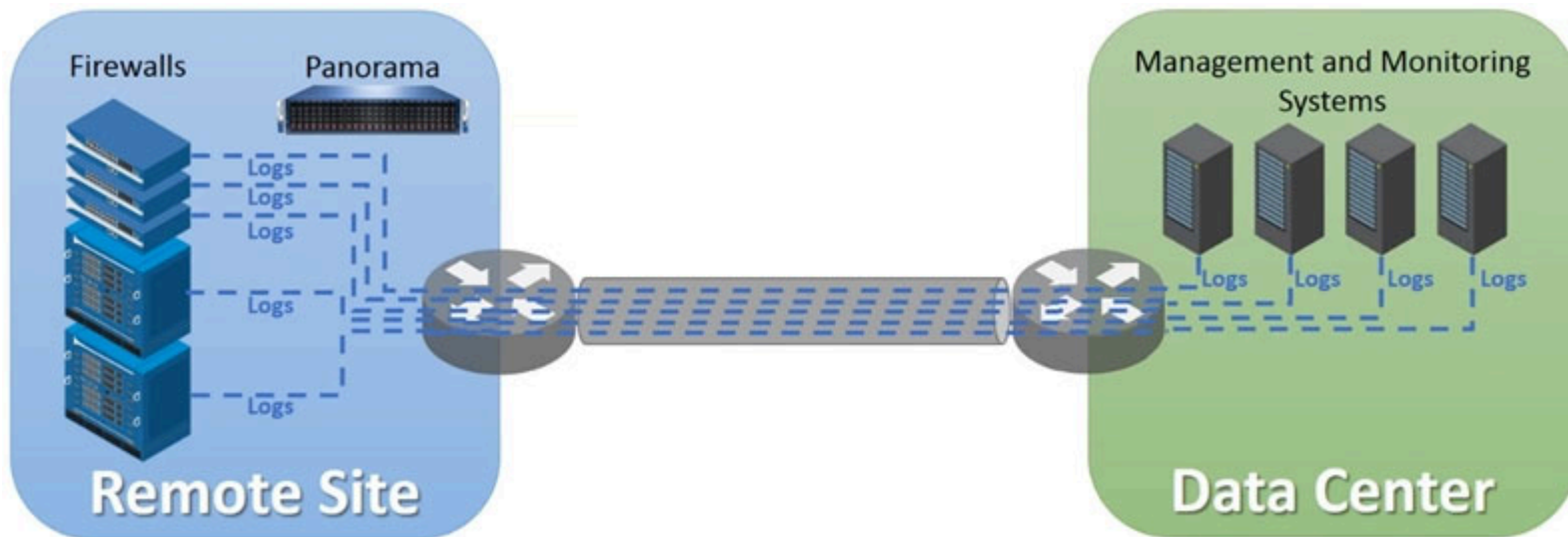
"test" command to test policy matches
upvoted 1 times

niklaus 2 years, 3 months ago

Selected Answer: C

Correct Answer: C
Link: <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-cli-quick-start/use-the-cli/test-the-configuration/test-policy-matches>
PAN-OS: 10.2
Time of answer: May 12, 2022
upvoted 1 times

Refer to the exhibit.



An organization has Palo Alto Networks NGFWs that send logs to remote monitoring and security management platforms. The network team has reported excessive traffic on the corporate WAN.

How could the Palo Alto Networks NGFW administrator reduce WAN traffic while maintaining support for all the existing monitoring/security platforms?

- A. Forward logs from firewalls only to Panorama and have Panorama forward logs to other external services.
- B. Forward logs from external sources to Panorama for correlation, and from Panorama send them to the NGFW.
- C. Configure log compression and optimization features on all remote firewalls.
- D. Any configuration on an M-500 would address the insufficient bandwidth concerns.

Correct Answer: A

Adamabdi Highly Voted 3 years, 5 months ago

A is the correct

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIKFCA0>

upvoted 15 times

tomsui44 Highly Voted 3 years, 4 months ago

there is no means to compress logs leaving the firewall AFAIK. Since all the data has to traverse the WAN link neither of the solutions will help reducing the log volume.

I could imagine that they want to hear answer **A** though, but it rarely makes sense to me.

upvoted 5 times

CISCO101 Most Recent 2 weeks, 4 days ago

Is there anyone done exam recently? Just wonder if the questions still valid and answer is right.

upvoted 1 times

scanossa 7 months, 2 weeks ago

Selected Answer: A

Based on documentation correct answer is A:

Forward logs from firewalls to Panorama and from Panorama to external services—This configuration is best for deployments in which the connections between firewalls and external services have insufficient bandwidth to sustain the logging rate, which is often the case when the connections are remote. This configuration improves firewall performance by offloading some processing to Panorama.

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/centralized-logging-and-reporting/log-forwarding-options>

upvoted 1 times

Marshpillowz 7 months, 2 weeks ago

Selected Answer: A

Answer A makes most sense to me.

upvoted 1 times

lol12 1 year, 10 months ago

Selected Answer: A

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIKFCA0>

<https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/panorama-overview/centralized-logging-and-reporting/log-forwarding-options.html>


upvoted 1 times

[-]  **TAKUM1y** 1 year, 11 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/centralized-logging-and-reporting/log-forwarding-options>

upvoted 1 times

[-]  **MyKasala** 2 years, 1 month ago

Selected Answer: A

A is correct


upvoted 1 times

[-]  **anbohm** 2 years, 2 months ago

Selected Answer: A

Need to be A

upvoted 1 times

[-]  **Meko** 2 years, 2 months ago

Selected Answer: A

Firewall logs -> Panorama -> Monitoring system

upvoted 1 times

[-]  **rquintana** 2 years, 3 months ago

Selected Answer: A

After reading the KB, I vote for option A.

upvoted 1 times

[-]  **niklaus** 2 years, 3 months ago

Selected Answer: A

Correct Answer: A

Link: <https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/centralized-logging-and-reporting/log-forwarding-options>

PAN-OS: 10.2

Time of answer: May 30, 2022


upvoted 4 times

[-]  **Abu_Muhammad** 2 years, 4 months ago

Selected Answer: A

It is A

upvoted 2 times

[-]  **king04** 2 years, 6 months ago

Selected Answer: A

A is correct

upvoted 3 times

[-]  **tururu1496** 2 years, 6 months ago

Selected Answer: A


Answer: A

upvoted 3 times

[-]  **NNgiggs** 2 years, 7 months ago

the correct answer is A. forwarding from Panorama reduces the number of log streams and cut down extra negotiation traffic per stream etc.

upvoted 3 times

[-]  **deha** 2 years, 7 months ago

A is correct

upvoted 2 times

A customer wants to set up a VLAN interface for a Layer 2 Ethernet port.
Which two mandatory options are used to configure a VLAN interface? (Choose two.)

- A. Virtual router
- B. Security zone
- C. ARP entries
- D. Netflow Profile

Correct Answer: CD

  **Edu147** Highly Voted 5 years, 1 month ago
Correct A, B

Configure Netflow profile is not mandatory
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRqCAK>
upvoted 14 times

  **StevenWilliams0728** Most Recent 4 months ago

I feel like this is one of those trick questions....You can create an interface that is marked as layer 2 type and it does not need an IP address. Just because it says vlan interface doesnt mean its layer 3 routable.



When walking through my palo none of these items are "required" when I create a physical interface and mark as a layer 2 vlan.
upvoted 1 times

  **b8c290d** 4 months, 1 week ago

To configure a VLAN interface for a Layer 2 Ethernet port, the two mandatory options you need to set are:

- A. Virtual router - This specifies which virtual router the VLAN interface is associated with. The virtual router handles the routing of traffic entering and leaving the VLAN.
- B. Security zone - This option assigns the VLAN interface to a specific security zone. Security zones are used to control and manage traffic based on the security policies defined within the firewall.

Options C (ARP entries) and D (Netflow Profile) are not mandatory for configuring a VLAN interface. ARP entries are automatically managed by the device as needed, and a Netflow Profile is related to traffic monitoring, not a basic configuration requirement for setting up a VLAN interface.
upvoted 1 times



  **utahman3431** 6 months ago

Selected Answer: AB

This plus an IP address was all I used to configure my VLANs.
upvoted 1 times

  **StevenWilliams0728** 5 months ago

You do not need an IP address for a "layer 2" vlan.
upvoted 1 times

  **zulu21** 7 months, 1 week ago

Selected Answer: BC

Correct B and C
Layer 2, no mandatory virtual router(Layer 3) and not netflow profile
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRqCAK>
upvoted 1 times

  **StevenWilliams0728** 5 months ago

But you don't need ARP entries either.....
upvoted 1 times

  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: AB



Correct answer is A and B.

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/configure-interfaces/layer-2-interfaces/configure-a-layer-2-interface-subinterface-and-vlan>
upvoted 1 times

  **StevenWilliams0728** 5 months ago

You link never mentions the need for a virtual router....



upvoted 1 times

  **killuillu** 7 months, 3 weeks ago

Selected Answer: AB

Correct A,B

upvoted 1 times

  **StevenWilliams0728** 9 months, 2 weeks ago

Selected Answer: AB

Strange the answer is listed as C,D



upvoted 2 times

  **Nikita0806** 11 months, 3 weeks ago

Selected Answer: CD

I select these option due to the fact that layer 2 interface configuration in Palo, as we select layer 2 in interface it never ask for Virtual router.

upvoted 1 times

  **JRKhan** 7 months, 4 weeks ago

The question refers to a vlan interface which is essentially used to provide L3 connectivity for a vlan. In order to configure vlan interface, you have to provide security zone and virtual router within the configuration.

upvoted 2 times

  **troiansmaxx** 1 year, 3 months ago

Selected Answer: AB

Answer is A,B

upvoted 1 times

  **mercysayno765** 1 year, 3 months ago

Selected Answer: AB

Virtual Router and Security Zone

upvoted 1 times

  **[Removed]** 1 year, 5 months ago

Selected Answer: AB

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/network/network-interfaces-vlan>

upvoted 2 times

  **kewokil120** 1 year, 5 months ago

Selected Answer: AB

Correct A, B

upvoted 1 times

  **Questionario** 1 year, 5 months ago

Selected Answer: AB

none of those are mandatory but the first two are the most plausible answers as those need to be configured for the interface to work



upvoted 2 times

  **Mauz88** 1 year, 7 months ago

Selected Answer: AB

A and B



upvoted 1 times

  **lol12** 1 year, 10 months ago

A, B

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRqCAK>

upvoted 2 times

  **bartgb** 1 year, 10 months ago

Selected Answer: AB

A and B

upvoted 2 times

An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against worms and trojans. Which Security Profile type will protect against worms and trojans?

- A. Anti-Spyware
- B. Instruction Prevention
- C. File Blocking
- D. Antivirus

Correct Answer: D

Reference:



<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/security-profiles>

  **rajputparveen** Highly Voted 4 years, 3 months ago

D is the correct
upvoted 9 times

  **thelittleyellowbirdie** Most Recent 3 weeks, 2 days ago

Antivirus profiles to protect against worms, viruses, and trojans and to block spyware downloads.
URL filtering profiles to restrict users access to specific websites and/or website categories, such as shopping or gambling
File blocking profiles to block selected file types, and in the specified session flow direction (inbound/outbound/both)
WildFire™ analysis profiles to specify for file analysis to be performed locally on the WildFire appliance or in the WildFire cloud
Data filtering profiles that help prevent sensitive information such as credit card or social security numbers from leaving a protected network
DoS Protection profiles are used with DoS Protection policy rules to protect the firewall from high-volume single-session and multiple-session attacks.
GTP Protection profiles enables the firewall to inspect, validate and filter GTP traffic
upvoted 1 times

  **zulu21** 7 months, 1 week ago

Selected Answer: D

Correct D
upvoted 1 times



  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: D

D is the correct answer.

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/security-profiles>



upvoted 1 times

  **mercysayno765** 1 year, 3 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-security-profiles>

upvoted 1 times

  **lol12** 1 year, 10 months ago

Selected Answer: D

D
<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/security-profiles>

upvoted 3 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/security-profiles>

upvoted 1 times

  **DriVen** 2 years, 1 month ago

INSTRUCTION prevention....lol

upvoted 1 times


  **niklaus** 2 years, 3 months ago

Selected Answer: D

Correct Answer: D

Link: <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/security-profiles>

PAN-OS: 10.2
Time of answer: May 30, 2022
upvoted 3 times


  **king04** 2 years, 6 months ago

Selected Answer: D

D is correct
upvoted 1 times

  **jianghaoxiang** 3 years ago

Answer: D
upvoted 2 times

  **dgetaneh** 3 years, 3 months ago

D is correct,
<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/policy/security-profiles.html>
upvoted 1 times

  **rocioha** 3 years, 5 months ago

D is the correct Answer: <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles>
ntivirus profiles protect against viruses, worms, and trojans as well as spyware downloads
upvoted 2 times

  **theroghert** 3 years, 6 months ago



only D
upvoted 1 times

  **DocHoliday** 3 years, 6 months ago



Anti virus profile protects against viruses and worms.
Anti spyware prevents them from contacting the outside world. (call home)
upvoted 1 times

  **Laurence64** 3 years, 9 months ago

D is correct
upvoted 2 times

  **lol1000** 3 years, 10 months ago

Answer: A
Latest ref:
<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/policy/security-profiles.html>
upvoted 2 times

  **renegade_xt** 3 years, 8 months ago

your ref says : "Antivirus profiles protect against viruses, worms, and trojans as well as spyware downloads."
upvoted 2 times

A company needs to preconfigure firewalls to be sent to remote sites with the least amount of preconfiguration. Once deployed, each firewall must establish secure tunnels back to multiple regional data centers to include the future regional data centers.

Which VPN configuration would adapt to changes when deployed to the future site?

- A. Preconfigured GlobalProtect satellite
- B. Preconfigured GlobalProtect client
- C. Preconfigured IPsec tunnels
- D. Preconfigured PPTP Tunnels

Correct Answer: A

  **327c7c8** 5 months, 1 week ago

Selected Answer: A

A: <https://knowledgebase.paloaltonetworks.com/kCSArticleDetail?id=kA10g000000CIEQ>
upvoted 1 times

  **Marshpillowz** 7 months, 2 weeks ago

A is the correct answer.

<https://knowledgebase.paloaltonetworks.com/kCSArticleDetail?id=kA10g000000CIEQ>
upvoted 1 times



  **dtisolutions** 1 year ago

A
<https://knowledgebase.paloaltonetworks.com/kCSArticleDetail?id=kA10g000000CIEQ#:~:text=GlobalProtect%20Satellite%20simplifies%20the%20deployment,on%20the%20remote%20satellite%20devices>
upvoted 1 times

  **Emanc21** 1 year, 8 months ago

Selected Answer: A

A is correct.
upvoted 1 times

  **lol12** 1 year, 10 months ago

A
<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/large-scale-vpn-lsvpn/configure-the-globalprotect-portal-for-lsvpn/define-the-satellite-configurations>
upvoted 3 times

  **TAKUM1y** 1 year, 11 months ago


Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/large-scale-vpn-lsvpn/configure-the-globalprotect-portal-for-lsvpn/define-the-satellite-configurations>
upvoted 1 times

  **niklaus** 2 years, 3 months ago

Selected Answer: A

Correct Answer: A
Link: <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/large-scale-vpn-lsvpn/configure-the-globalprotect-portal-for-lsvpn/define-the-satellite-configurations>
PAN-OS: 10.2
Time of answer: May 30, 2022
upvoted 1 times

  **king04** 2 years, 6 months ago

Selected Answer: A

A is correct
upvoted 3 times

  **theroghert** 3 years, 6 months ago

only A
upvoted 3 times

  **lol1000** 3 years, 10 months ago

Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/large-scale-vpn-lsvpn/configure-the-globalprotect-portal-for-lsvpn/define-the-satellite-configurations.html>

upvoted 3 times

  **nk12** 4 years ago



Correct Answer: A

upvoted 2 times

  **rajputparveen** 4 years, 3 months ago

A is right answer

upvoted 1 times

  **johnte** 4 years, 4 months ago

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/large-scale-vpn-lsvpn/configure-the-globalprotect-portal-for-lsvpn/define-the-satellite-configurations>

upvoted 3 times

An administrator has been asked to configure active/passive HA for a pair of Palo Alto Networks NGFWs. The administrator assigns priority 100 to the active firewall.

Which priority is correct for the passive firewall?

- A. 0
- B. 99
- C. 1
- D. 255

Correct Answer: D

Reference:

<https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/high-availability/device-priority-and-preemption>

Yasi Highly Voted 4 years, 1 month ago

The lower the number, the higher the priority.

So if active is higher priority, therefore assigned 100, then the only one that will be second priority will be with number larger than 100 so Only 255 is applicable. Therefore D is the correct answer.

upvoted 16 times

StevenWilliams0728 Most Recent 5 months ago

The firewalls in an Active-Passive HA pair can be assigned a device priority value to indicate a preference for which firewall should assume the active role. If you need to use a specific firewall in the HA pair for actively securing traffic, you must enable the preemptive behavior on both the firewalls and assign a device priority value for each firewall. The firewall with the lower numerical value, and therefore higher priority, is designated as active. The other firewall is the passive firewall.

upvoted 1 times

327c7c8 5 months, 1 week ago

Selected Answer: D

D: lower numeric value is higher priority

upvoted 1 times

Marshpillowz 7 months, 2 weeks ago

Selected Answer: D

The only answer it can be is D.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/ha-concepts/device-priority-and-preemption>

upvoted 1 times

easylife 10 months, 2 weeks ago

Selected Answer: D

D is correct:

I gave the Palo-Alto-Networks PCNSA test and scored 910/1000. This was all possible because of marks4sure as it helped me to pass in the first attempt.

upvoted 1 times

lol12 1 year, 10 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/device-priority-and-preemption>

upvoted 3 times

TAKUM1y 1 year, 11 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/device-priority-and-preemption>

upvoted 1 times

niklaus 2 years, 3 months ago

Selected Answer: D

Correct Answer: D

Link: <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/device-priority-and-preemption>



PAN-OS: 10.2



Time of answer: May 30, 2022



upvoted 2 times

KhalidB 2 years, 6 months ago

D IS CORRECT
upvoted 2 times



  **dgetaneh** 3 years, 3 months ago
D is correct
upvoted 3 times



  **theroghert** 3 years, 6 months ago
only D
upvoted 4 times



  **lol1000** 3 years, 10 months ago
Answer: D

Passive needs lower priority so higher number.

https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf page 315
upvoted 4 times

  **nk12** 4 years ago
Correct Answer: D
upvoted 2 times

  **Nib2002** 4 years, 1 month ago
The firewall you plan to make active must have a lower numerical value than its peer. So, if Peer A is to function as the active firewall, keep the default value of 100 and increment the value on PeerB.
upvoted 1 times

  **cloudguy365** 4 years, 4 months ago
firewall with the lower numerical value, and therefore higher priority, is designated as active.
upvoted 3 times

An administrator pushes a new configuration from Panorama to a pair of firewalls that are configured as an active/passive HA pair. Which NGFW receives the configuration from Panorama?

- A. The passive firewall, which then synchronizes to the active firewall
- B. The active firewall, which then synchronizes to the passive firewall
- C. Both the active and passive firewalls, which then synchronize with each other
- D. Both the active and passive firewalls independently, with no synchronization afterward

Correct Answer: D

— **Mohammed** Highly Voted 4 years, 4 months ago

I thinsk answer is D

<https://live.paloaltonetworks.com/t5/General-Topics/config-push-from-panorama-to-HA-PA/td-p/236297>

upvoted 14 times

— **oo7** Highly Voted 4 years, 4 months ago

D

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleOCAS>

upvoted 10 times

— **scanossa** Most Recent 7 months ago

Selected Answer: D

I set up a lab with an HA pair, both devices received the configuration in their respective template stack and then, performed a commit. Because the values are the same, no synchronization is needed.

upvoted 1 times

— **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: D

D is the correct answer.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleOCAS>

upvoted 2 times

— **evdw** 1 year, 8 months ago

Correct Answer is D

Policies and templates from Panorama must be committed to both active and passive HA devices! They are not getting synched!

upvoted 2 times

— **myname_1** 1 year, 8 months ago

Selected Answer: D

This has some info for migrating HA into Panorama:

<https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/manage-firewalls/transition-a-firewall-to-panorama-management/migrate-a-firewall-ha-pair-to-panorama-management>

Basically, Panorama configuration is not synced regardless of if the config sync box is checked. Only local configuration will be synchronized if the config sync box is checked.

upvoted 2 times

— **lol12** 1 year, 10 months ago

Selected Answer: D

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleOCAS>

upvoted 1 times

— **ashmeow** 2 years ago

Selected Answer: D

Sync only happens if you commit locally and enable config sync is ticked under the HA section

upvoted 1 times

— **melek18** 2 years, 1 month ago

Selected Answer: C

In my opinion C

upvoted 1 times

— **ThatIT** 2 years, 3 months ago

The Correct answer here is C , both firewalls will receive the configuration and will need to sync what the configuration it is, may be an application , objects ,security policy . On panorama you will also see on the devices it will show they are in-sync or out of sync


upvoted 1 times

  **king04** 2 years, 6 months ago

Selected Answer: D

D is correct

upvoted 1 times

  **r0ze** 2 years, 10 months ago

Answer: D

upvoted 2 times

  **uNburNed** 3 years, 2 months ago

Should be C

upvoted 2 times

  **Breyarg** 2 years, 8 months ago



no its D. although we always set up HA with sync enabled, its not a requirement for HA. so just HA without the "additional and optional" sync, will not sync.

upvoted 1 times

  **theroghert** 3 years, 6 months ago



only D

upvoted 1 times

  **Sarbi** 3 years, 9 months ago

Ths answer is D

upvoted 1 times

  **lol1000** 3 years, 10 months ago

Answer: D

sk suggests that Panorama policy is pushed to both units and no sync is performed per se. This means that any local policy would need to be synced separately

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleOCAS>

upvoted 1 times

  **guilherme_a** 3 years, 12 months ago

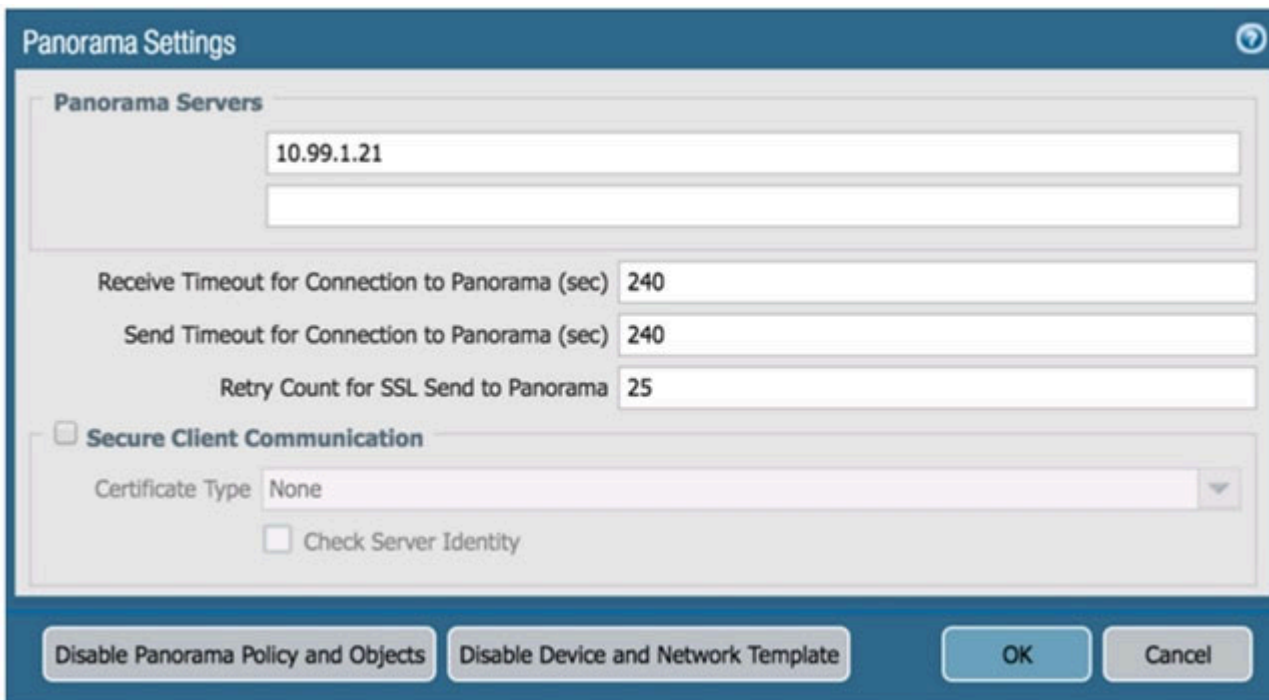
D is correct

upvoted 1 times

An administrator cannot see any Traffic logs from the Palo Alto Networks NGFW in Panorama reports. The configuration problem seems to be on the firewall.

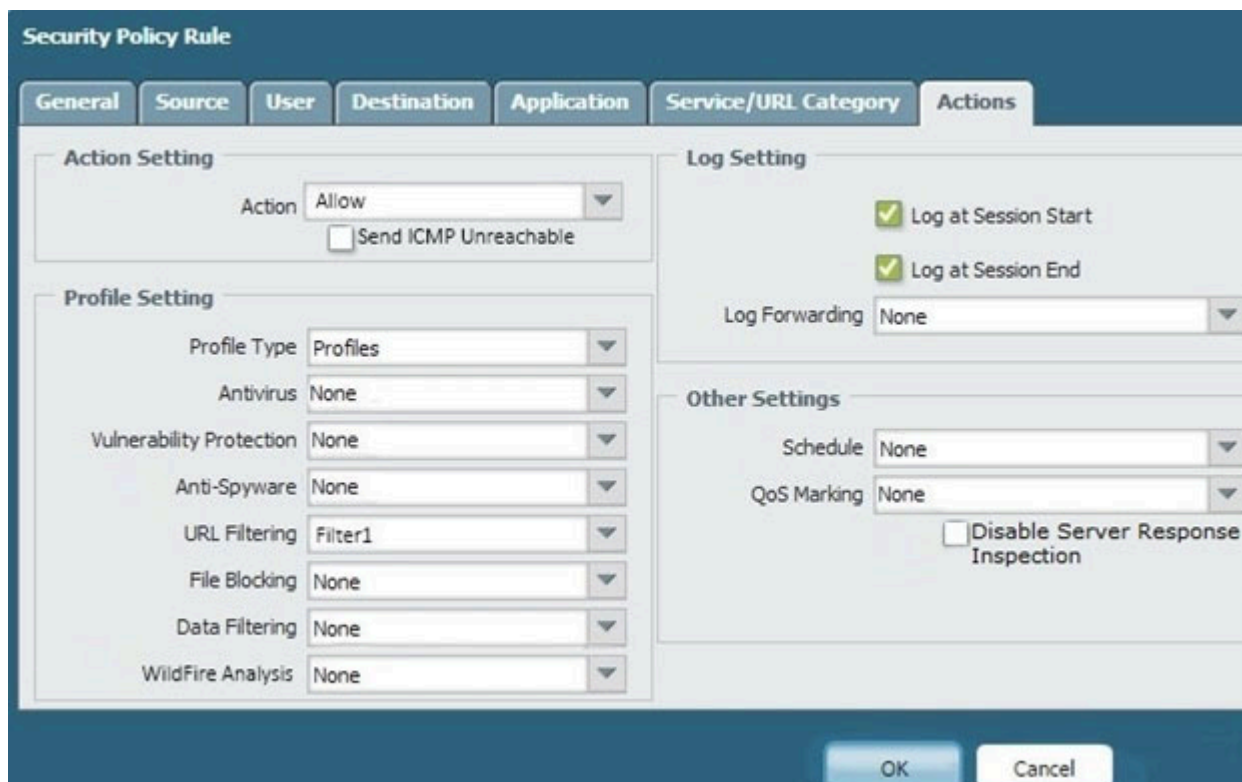
Which settings, if configured incorrectly, most likely would stop only Traffic logs from being sent from the firewall to Panorama?

A.



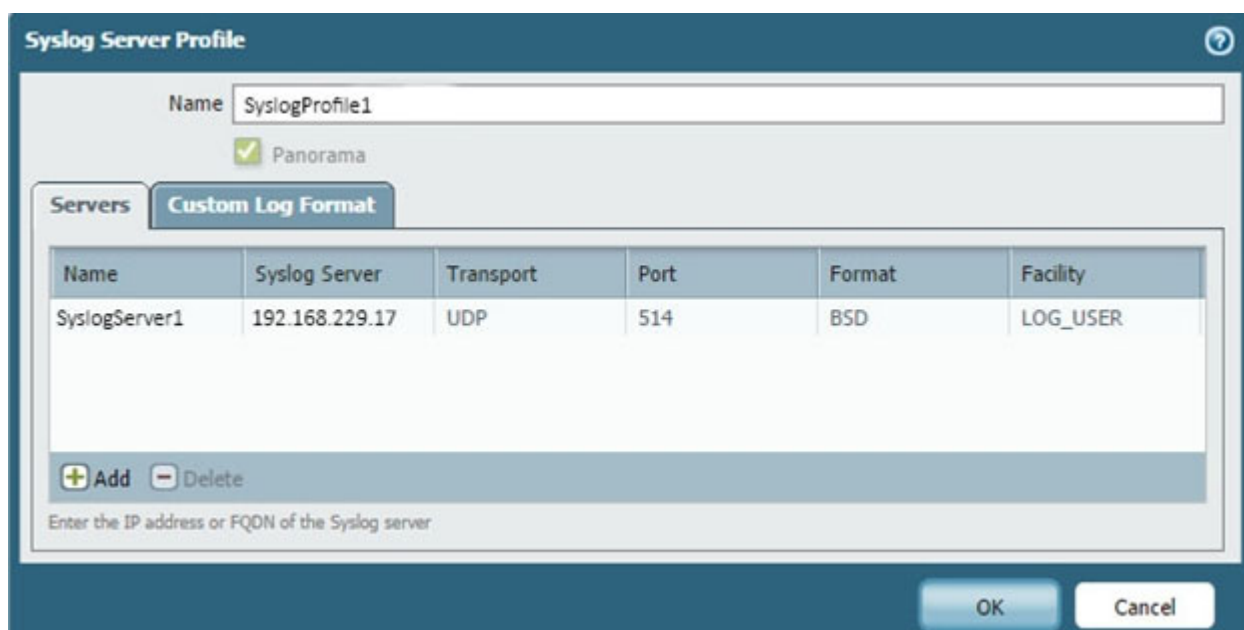
The screenshot shows the 'Panorama Settings' window. Under the 'Panorama Servers' section, the IP address '10.99.1.21' is entered. Below this, the 'Receive Timeout for Connection to Panorama (sec)' is set to 240, the 'Send Timeout for Connection to Panorama (sec)' is set to 240, and the 'Retry Count for SSL Send to Panorama' is set to 25. In the 'Secure Client Communication' section, the 'Certificate Type' is set to 'None' and the 'Check Server Identity' checkbox is unchecked. At the bottom, there are buttons for 'Disable Panorama Policy and Objects', 'Disable Device and Network Template', 'OK', and 'Cancel'.

B.

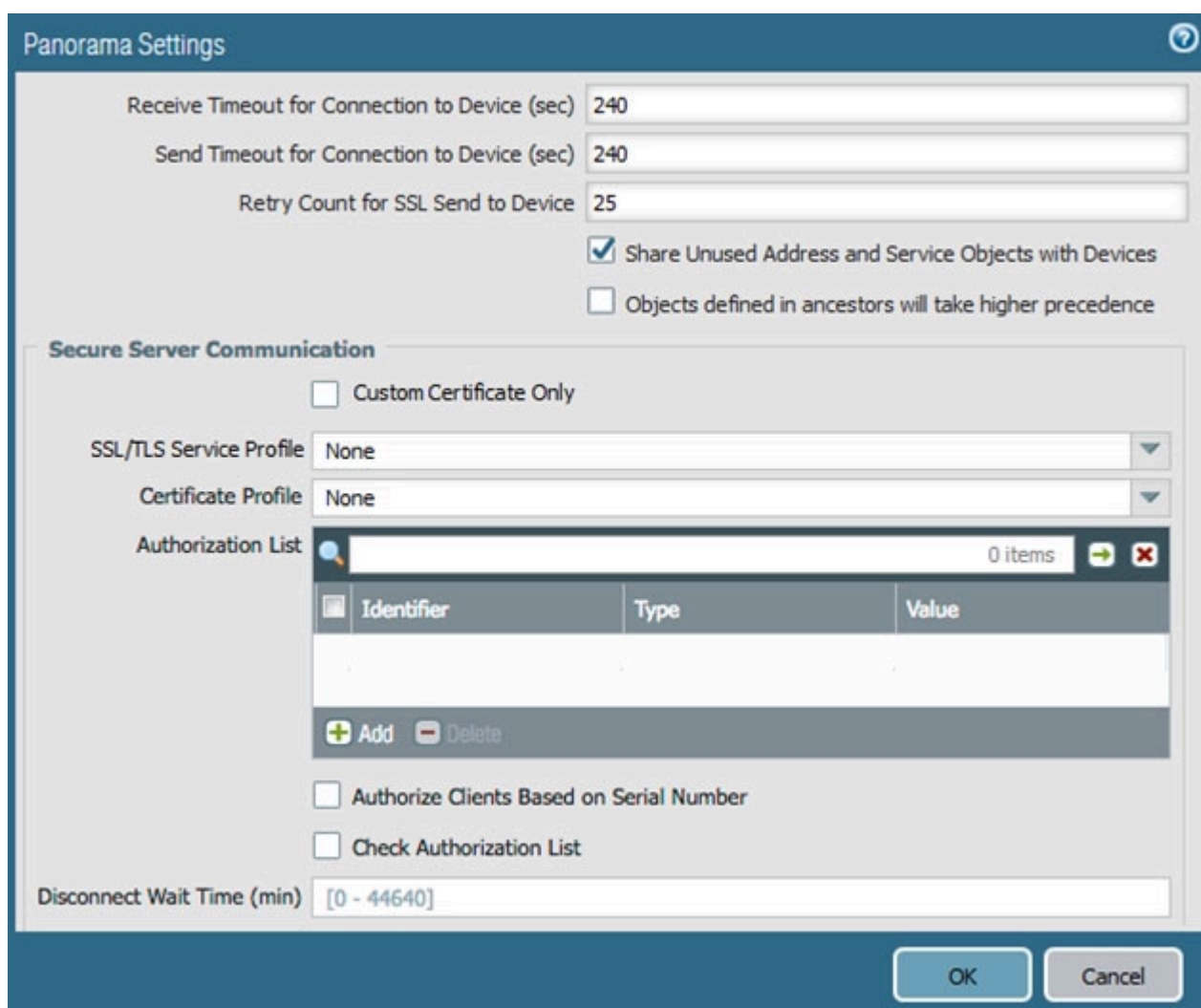


The screenshot shows the 'Security Policy Rule' configuration window, specifically the 'Actions' tab. Under 'Action Setting', the 'Action' is set to 'Allow' and the 'Send ICMP Unreachable' checkbox is unchecked. Under 'Profile Setting', various profile types are set to 'None' or 'Filter1'. Under 'Log Setting', 'Log at Session Start' and 'Log at Session End' are checked, and 'Log Forwarding' is set to 'None'. Under 'Other Settings', 'Schedule' and 'QoS Marking' are set to 'None', and the 'Disable Server Response Inspection' checkbox is unchecked. At the bottom, there are 'OK' and 'Cancel' buttons.

C.



D.



Correct Answer: B

shetoshandasa Highly Voted 3 years, 5 months ago

The answer is B.
Log forwarding in the right is shown "None", Log forwarding profile should be selected.
upvoted 13 times

zerox7305 Highly Voted 2 years, 8 months ago

B is the Answer 100%
upvoted 8 times

BTSeeYa Most Recent 1 month, 3 weeks ago

Not sure why everyone is picking B. That's config for one rule, not the entire firewall, and there's a URL-Filtering profile added. URL-Filtering logs are different than "only Traffic logs". Look at at the post above which mentioned C and also notice Panorama is checked.
upvoted 1 times

hcir 2 months, 3 weeks ago



























it is definitely B. Security Profiles are not set, so no threat logs can be sent. And there is not log forwarding profile, so no traffic log either
upvoted 1 times

Marshpillowz 7 months, 2 weeks ago

Answer is B. There is no log forwarding profile configured.
upvoted 1 times

90fa8d0 8 months, 1 week ago

A + B. there is another diagram not shown on that question.
https://vceguide.com/wp-content/uploads/2018/10/PALO-ALTO-NETWORKS-PCNSE-DATA-10012018_06_Image_0001.jpg
upvoted 1 times

-   **Woody** 1 year, 8 months ago
If the traffic log checkbox was not checked when creating the log forwarding profile, other logs will be sent but traffic log. I vote for B.
upvoted 1 times
-   **lol12** 1 year, 10 months ago
It is A. This question is missing network diagram with Panorama IP address 10.99.1.2
upvoted 1 times
-   **ashmeow** 2 years ago
I think it should be B. There is no need to select a certificate, you can just use predefined, so I think that rules out D.
upvoted 1 times
-   **JMIB** 2 years ago
B is the Answer 100%
upvoted 1 times
-   **rquintana** 2 years, 2 months ago
I vote for option B, if the log forwarding profile is None, any logs will be sent to Panorama.
upvoted 1 times
-   **ChinkSantana** 2 years, 2 months ago
Are you planning to take the exam soon? Have you found any other materials beside from this? I plan to take by end of June
upvoted 1 times
-   **Meko** 2 years, 2 months ago
B - forgot to set the Log Forwarding Profiles
upvoted 1 times
-   **ThatIT** 2 years, 3 months ago
Log Forwarding
upvoted 1 times
-   **nostal** 2 years, 4 months ago
B & D both showing incorrect configuration, as in B we see log forwarding profiles set to none which means no syslog traffic will be sent, while in D we can no cert file selected for Panorama communication, but B may be better as it "would stop only Traffic logs"
upvoted 2 times
-   **Frightened_Acrobat** 2 years, 4 months ago
B does make the most sense. A Log Forwarding profile can be configured to filter out certain logs using the Filter Builder.
upvoted 2 times
-   **Frightened_Acrobat** 2 years, 4 months ago
Consider option C. This question is still on the PCNSE exam. I've seen it come up twice. I don't know that I'm getting it correct by choosing B. The question specifically says only Traffic logs are missing. If the Log Forwarding Profile is missing, this would affect Threat logs as well. In option C, there is a Syslog server. If you see the "Custom Log Format," you can change just the format for Traffic logs and this could break how Panorama ingests those logs. I couldn't find anything on Palo Alto networks sites, but here's forum where a Palo Alto user was having a similar issue with Splunk. <https://community.splunk.com/t5/All-Apps-and-Add-ons/Custom-Log-Format-Parsing-issues/m-p/548818>
upvoted 3 times
-   **gfontenot10** 2 years, 4 months ago
I get the question, but syslog are normally for external monitoring like Splunk or Solarwinds. The Logging forwarding profile must be configured and it is set to none right now. Under log forwarding you can set different profiles for each log type - threat, traffic etc. This is where the answer really should be.
upvoted 4 times
-   **AbuHussain** 2 years, 5 months ago
The answer is B.
upvoted 2 times

When configuring a GlobalProtect Portal, what is the purpose of specifying an Authentication Profile?

- A. To enable Gateway authentication to the Portal
- B. To enable Portal authentication to the Gateway
- C. To enable user authentication to the Portal
- D. To enable client machine authentication to the Portal

Correct Answer: C

The additional options of Browser and Satellite enable you to specify the authentication profile to use for specific scenarios. Select Browser to specify the authentication profile to use to authenticate a user accessing the portal from a web browser with the intent of downloading the GlobalProtect agent (Windows and Mac). Select Satellite to specify the authentication profile to use to authenticate the satellite.

Reference -

<https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/globalprotect/network-globalprotect-portals>

  **Shahi** Highly Voted 4 years, 3 months ago

Correct C
upvoted 11 times

  **a43b1bf** Most Recent 1 day, 12 hours ago

Selected Answer: C
Answer C
upvoted 1 times

  **kambata** 2 months ago

Selected Answer: C
C, of course
upvoted 1 times

  **Marshpillowz** 7 months, 2 weeks ago



Selected Answer: C
Answer is C.

<https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin/globalprotect-portals/set-up-access-to-the-globalprotect-portal>
upvoted 1 times

  **dorf05** 9 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin/globalprotect-portals/define-the-globalprotect-client-authentication-configurations#:~:text=Each%20GlobalProtect%20client%20authentication%20configuration%20specifies%20the%20settings%20that%20enable%20the%20user%20to%20authenticate%20with%20the%20GlobalProtect%20portal>
upvoted 1 times



  **PANW** 1 year, 8 months ago

Selected Answer: D



I am not sure that C is the right answer
<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/globalprotect/network-globalprotect-portals/globalprotect-portals-authentication-configuration-tab>

In addition to distinguishing a client authentication configuration by an OS, you can further differentiate by specifying an authentication profile. (You can create a New Authentication Profile or select an existing one.) To configure multiple authentication options for an OS, you can create multiple client authentication profiles.

upvoted 1 times

  **javim** 1 year, 7 months ago

Machine authentication is in pre-logout option. In this case is user authentication, C is the correct.
upvoted 2 times

  **PANW** 1 year, 8 months ago

Selected Answer: D

I am not sure that C is the right answer

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/globalprotect/network-globalprotect-portals/globalprotect-portals-authentication-configuration-tab>

In addition to distinguishing a client authentication configuration by an OS, you can further differentiate by specifying an authentication profile. (You can create a New Authentication Profile or select an existing one.) To configure multiple authentication options for an OS, you can create multiple client authentication profiles.


upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-portals/define-the-globalprotect-client-authentication-configurations>


upvoted 3 times

  **UFanat** 2 years, 2 months ago

Selected Answer: C

C is Correct. First user should be authenticated on Portal.

upvoted 2 times

  **king04** 2 years, 6 months ago

Selected Answer: C



C is correct

upvoted 2 times

  **theroghert** 3 years, 6 months ago

only C

upvoted 2 times

  **lol1000** 3 years, 10 months ago



Answer: c

Users authenticate to the portal...

Each GlobalProtect client authentication configuration specifies the settings that enable the user to authenticate with the GlobalProtect portal.

<https://docs.paloaltonetworks.com/globalprotect/10-0/globalprotect-admin/globalprotect-portals/define-the-globalprotect-client-authentication-configurations.html>

upvoted 4 times

  **nk12** 4 years ago

Correct Answer: C

upvoted 2 times

If a template stack is assigned to a device and the stack includes three templates with overlapping settings, which settings are published to the device when the template stack is pushed?

- A. The settings assigned to the template that is on top of the stack.
- B. The administrator will be prompted to choose the settings for that chosen firewall.
- C. All the settings configured in all templates.
- D. Depending on the firewall location, Panorama decides with settings to send.

Correct Answer: A

  **Edu147** Highly Voted 5 years, 1 month ago
Correct A

If templates have duplicate settings, Panorama will push only the settings of the higher template in the list to the assigned firewalls
<https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/panorama-web-interface/panorama-templates/template-stacks>
upvoted 15 times

  **scanossa** Most Recent 7 months, 2 weeks ago

Selected Answer: A

After doing a lab we confirmed the template located on top has the priority
upvoted 1 times

  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: A

Top-down - correct answer is A.
upvoted 1 times



  **Questionario** 1 year, 5 months ago

A, unless configured the other way around
upvoted 1 times

  **mbhuyan** 1 year, 6 months ago

Selected Answer: A

Top-down hierarchy --
Correct Answer: A
upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/templates-and-template-stacks>
upvoted 2 times



  **UFanat** 2 years, 2 months ago

Selected Answer: A



top down priority
upvoted 2 times

  **KhalidB** 2 years, 6 months ago

THE ANSWER IS A
upvoted 3 times


  **DDDaaa2021** 2 years, 10 months ago

Failed exam today. A lot of new questions not on this dump. This would be new v10 exam.
1. 3-4 port mirror questions
2. Over 5 sd-wan questions
3. 3-5 prisma questions
4. Approx 10 new panorama questions.
5. 3 new drag n drops
6. 5 new plan questions.
Has anyone else done this exam recently?
upvoted 3 times

  **Bighize** 2 years, 9 months ago

Agreed. Failed Exam today. Only had about 8 questions from this dump. They are shifting to focus to Panaorama Deployment, Device Groups and Template stacks, UserID and mapping, Certificate questions and SSL decryption and SD-WAN. There is some Prisma on there, as well. You may not pass if you rely on this.

upvoted 2 times

  **r0ze** 2 years, 10 months ago

Correct Answer: A

upvoted 2 times

  **rocioha** 3 years, 5 months ago



Agree is A

upvoted 1 times

  **theroghert** 3 years, 6 months ago



only A

upvoted 1 times

  **Ali526** 3 years, 8 months ago

I just started using this site. I don't get this: everyone in this discussion agrees that the correct answer is A, and I also agree that it is A (after reading PA guide), then why the answer in "Reveal..." is B. Who gave them the wrong answer and why cannot they fix. Many of the members here are very knowledgeable and experienced.

upvoted 4 times

  **nk12** 4 years ago

Correct Answer: A

upvoted 2 times

  **bnilam2** 4 years, 2 months ago



Correct Answer is A

upvoted 2 times

  **bnilam2** 4 years, 3 months ago

Correct is A

upvoted 3 times

  **Shahi** 4 years, 3 months ago

Correct is A

upvoted 2 times

Which method will dynamically register tags on the Palo Alto Networks NGFW?

- A. Restful API or the VMware API on the firewall or on the User-ID agent or the ready-only domain controller (RODC)
- B. Restful API or the VMware API on the firewall or on the User-ID agent
- C. XML API or the VMware API on the firewall or on the User-ID agent or the CLI
- D. XML API or the VM Monitoring agent on the NGFW or on the User-ID agent

Correct Answer: D

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/register-ip-addresses-and-tags-dynamically>

  **palolover** 7 months ago



D is the correct answer
upvoted 1 times

  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: D

Answer is D.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/register-ip-addresses-and-tags-dynamically>
upvoted 2 times

  **Sammy3637** 9 months ago

Selected Answer: D

PAN-OS XML API USAGE - read the topic from PA documentation
upvoted 1 times

  **dorf05** 9 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/policy/monitor-changes-in-the-virtual-environment/use-dynamic-address-groups-in-policy#:~:text=To%20dynamically%20register%20tags%2C%20you%20can%20use%20the%20XML%20API%20or%20the%20VM%20Monitoring%20agent%20on%20the%20firewall%20or%20on%20the%20User%2DID%20agent.>
upvoted 1 times

  **GohanF2** 1 year, 7 months ago

it will be D . Reference: <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/register-ip-addresses-and-tags-dynamically>
upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/monitor-changes-in-the-virtual-environment/use-dynamic-address-groups-in-policy>
upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: D

D is a correct one
<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/policy/monitor-changes-in-the-virtual-environment/use-dynamic-address-groups-in-policy.html>
upvoted 2 times

  **SMahaldar** 3 years, 1 month ago

D only
upvoted 2 times



  **achille5** 3 years, 5 months ago

Correct is D
XML API—The firewall and Panorama support an XML API that uses standard HTTP requests to send and receive data. You can use this API to register IP addresses and tags with the firewall or Panorama. API calls can be made directly from command line utilities such as cURL or using any scripting or application framework that supports REST-based services. Refer to the PAN-OS XML API Usage Guide for details.
upvoted 1 times

  **theroghert** 3 years, 6 months ago

only D



upvoted 2 times

  **lol1000** 3 years, 10 months ago

Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/policy/monitor-changes-in-the-virtual-environment/use-dynamic-address-groups-in-policy.html>

upvoted 3 times

  **nk12** 4 years ago

Correct Answer: D

To dynamically register tags, you can use the XML API or the VM Monitoring agent on the firewall or on the User-ID agent.

upvoted 1 times

  **bnilam2** 4 years, 2 months ago

D is correct

upvoted 1 times

  **alpha520** 4 years, 3 months ago

D is correct

upvoted 3 times

  **Jeevan1982** 4 years, 3 months ago

answer is D : <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/policy/register-ip-addresses-and-tags-dynamically>

upvoted 3 times



  **Ab121213** 4 years, 3 months ago

To dynamically register tags, you can use the XML API or the VM Monitoring agent on the firewall or on the User-ID agent

D is correct.

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/policy/monitor-changes-in-the-virtual-environment/use-dynamic-address-groups-in-policy>

upvoted 2 times

  **Baig1** 4 years, 4 months ago

C is correct

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/cli-commands-for-dynamic-ip-addresses-and-tags.html>

upvoted 1 times

How does an administrator schedule an Applications and Threats dynamic update while delaying installation of the update for a certain amount of time?

- A. Configure the option for "Threshold".
- B. Disable automatic updates during weekdays.
- C. Automatically "download only" and then install Applications and Threats later, after the administrator approves the update.
- D. Automatically "download and install" but with the "disable new applications" option used.

Correct Answer: A

  **rocioha** Highly Voted 3 years, 5 months ago

A is the right answer. <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/software-and-content-updates/install-content-and-software-updates>

upvoted 8 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: A

Correct answer is A.

Enter how long after a release to wait before performing a content update in the Threshold (Hours) field. In rare instances, errors in content updates may be found. For this reason, you may want to delay installing new updates until they have been released for a certain number of hours.



upvoted 2 times

  **dorf05** 9 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/device/device-dynamic-updates#:~:text=For%20Antivirus%20and,modified%20applications%20introduce>.

upvoted 1 times

  **lol12** 1 year, 10 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/device/device-dynamic-updates>

upvoted 1 times

  **ashmeow** 2 years ago

None of the options are perfect in my opinion. There are two thresholds that can be set in a schedule - Threshold (hours) which is the time to wait when a new app and threat update is available before taking the action (download only or download and install) or New App-ID Threshold (hours) which delays the installation.



upvoted 2 times

  **tenebrox** 2 years, 2 months ago

Selected Answer: A

its only one possibility, its A

upvoted 1 times

  **Meko** 2 years, 2 months ago

Selected Answer: C

Threathold (hours) - A content update must be at least this many hours old for the action to be taken.

upvoted 1 times

  **asdasd123123iu** 2 years, 5 months ago

Threshold determines the amount of time the firewall waits before installing the latest content. Correct answer is A

upvoted 1 times

  **confusion** 2 years, 6 months ago

Selected Answer: A

A, as the question asks for delaying the whole update:



<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/software-and-content-updates/best-practices-for-app-and-threat-content-updates/best-practices-mission-critical.html>

B is not relevant as it would disable the automatic updates.

C involves manual/admin action to install the update which is not "certain amount of time".

D would not delay the install of the content update, but disable the new Apps from it.

upvoted 3 times

  **rischa** 2 years, 6 months ago



Ans:C this for delayed installation for certain time. Ans: A is for the mission critical application availability 100% we can configure the threshold.
upvoted 2 times

  **confusion** 2 years, 6 months ago

Nope, A is correct and not related for mission critical only:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/software-and-content-updates/best-practices-for-app-and-threat-content-updates/best-practices-mission-critical.html>



upvoted 1 times

  **Igkhan** 2 years, 9 months ago

Selected Answer: A



A is correct.

upvoted 3 times

  **r0ze** 2 years, 10 months ago



Correct Answer: A

upvoted 2 times

  **r0ze** 2 years, 10 months ago

Correct Answer: A


upvoted 2 times

  **bluejl** 3 years, 1 month ago

C.

Threshold is to delay the Action, what if Action is "download-only"? which does not install updates at all, so A is wrong.

upvoted 2 times

  **Trung2735** 3 years ago

I think the question need to be worded more clearly. If it auto-install A, if it wait for approval C.

This is verbatim from their website.

"Schedule content updates so that they download-and-install automatically. Then, set a Threshold that determines the amount of time the firewall waits before installing the latest content. In a security-first network, schedule a six to twelve hour threshold."

upvoted 3 times

  **SMahaldar** 3 years, 1 month ago

A only

upvoted 1 times

  **kerberos** 3 years, 2 months ago

answer is A

upvoted 1 times

  **utahman3431** 3 years, 5 months ago

I would agree that this should be A

upvoted 2 times


To connect the Palo Alto Networks firewall to AutoFocus, which setting must be enabled?

- A. Device>Setup>Services>AutoFocus
- B. Device> Setup>Management >AutoFocus
- C. AutoFocus is enabled by default on the Palo Alto Networks NGFW
- D. Device>Setup>WildFire>AutoFocus
- E. Device>Setup> Management> Logging and Reporting Settings

Correct Answer: B

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-autofocus-threat-intelligence>

  **sethjam** Highly Voted 4 years, 2 months ago

Connect the firewall to AutoFocus.

1. Select Device> Setup> Management and edit the AutoFocus settings.

2. Enter the AutoFocus URL:

<https://autofocus.paloaltonetworks.com:10443>

upvoted 7 times

  **Ditzhak** Most Recent 5 months, 2 weeks ago

Selected Answer: B

Correct answer is B.

upvoted 1 times

  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: B

Correct answer is B.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/learn-more-about-and-assess-threats/assess-firewall-artifacts-with-autofocus/enable-autofocus-threat-intelligence>

upvoted 1 times

  **Xuzi** 10 months ago

Time to remove this question

upvoted 2 times

  **bobmead** 1 year, 2 months ago


No, Palo Alto Networks no longer uses AutoFocus. AutoFocus was discontinued on September 30, 2022. Palo Alto Networks has replaced AutoFocus with two new products:

Cortex XSOAR Threat Intelligence Management (TIM): This product provides a comprehensive threat intelligence management platform that includes features such as threat intelligence enrichment, threat intelligence correlation, and threat intelligence automation.

Cortex XDR (Extended Detection and Response): This product provides a unified endpoint security platform that includes features such as threat detection, threat investigation, and threat response.

Both Cortex XSOAR TIM and Cortex XDR include features that were previously available in AutoFocus. For example, both products can enrich threat intelligence with contextual information from Palo Alto Networks' threat intelligence feeds. Both products can also correlate threat intelligence to identify potential threats. And both products can automate threat response.

upvoted 4 times

  **Sudont** 1 year, 8 months ago

Very good chance that this will be removed soon as AutoFocus was EoS in September 2022.

upvoted 3 times

  **UFanat** 2 years, 2 months ago

Selected Answer: B

B is correct

1. Select Device> Setup> Management and edit the AutoFocus settings.

2. Enter the AutoFocus URL:

<https://autofocus.paloaltonetworks.com:10443>

upvoted 3 times

  **SMahaldar** 3 years, 1 month ago

B is right answer

upvoted 2 times

[-]  **achille5** 3 years, 6 months ago


B is the correct answer
upvoted 2 times

[-]  **CyberG** 3 years, 6 months ago

B is it
upvoted 3 times

[-]  **theroghert** 3 years, 6 months ago

only B
upvoted 2 times

[-]  **lol1000** 3 years, 10 months ago

Answer: B
Once you have license enabled new option will show in Device>Setup>Management

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/threat-prevention/learn-more-about-and-assess-threats/assess-firewall-artifacts-with-autofocus/enable-autofocus-threat-intelligence.html>

upvoted 4 times

[-]  **oshanp** 4 years ago

Answer B is correct
upvoted 1 times

[-]  **nk12** 4 years ago

Correct Answer: B
upvoted 2 times

[-]  **rajputparveen** 4 years, 3 months ago

B is correct
upvoted 3 times

An administrator encountered problems with inbound decryption. Which option should the administrator investigate as part of triage?

- A. Security policy rule allowing SSL to the target server
- B. Firewall connectivity to a CRL
- C. Root certificate imported into the firewall with `Trust` enabled
- D. Importation of a certificate from an HSM

Correct Answer: A

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssl-inbound-inspection>

BellaDrake Highly Voted 2 years, 7 months ago

The correct answer is A. Inbound decryption is where you are decrypting traffic to your internal server. You don't use a Root CA, you load that server's cert and private key. The Root cert is 'Optional'

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/configure-ssl-inbound-inspection.html>

upvoted 8 times

Marshpillowz Most Recent 7 months, 2 weeks ago

Selected Answer: A

Answer is A.

upvoted 1 times

beikenes 1 year, 8 months ago

It is worth mentioning that the policy needs to allow application identified when the SSL traffic is decrypted.

upvoted 1 times

lol12 1 year, 10 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-inbound-inspection>

upvoted 1 times

TAKUM1y 1 year, 10 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-inbound-inspection>

upvoted 1 times

spydog 1 year, 11 months ago

I will agree correct answer is A.

upvoted 1 times

spydog 1 year, 11 months ago

Initially I was leaning more to D, but I just realised it is misleading... Issues with HSM module could indeed cause inbound decryption problems, because HSM is used to store the private key. Without the private key FW cannot decrypt inbound traffic.

However HSM store the private key, while the certificate is imported once during the setup - <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/certificate-management/secure-keys-with-a-hardware-security-module/store-private-keys-on-an-hsm#idcaadcd26-7f7c-494a-bfaa-bdfb51826aec>

upvoted 1 times

spydog 1 year, 11 months ago

On other hand it is very important to understand the big difference between SSL Inbound Inspection and SSL Forward Proxy. With Inbound inspection firewall does not proxy the SSL session. Since it have the private key, client and server establish SSL directly with each other, while firewall can peak inside the encrypted traffic - because it has the private key for the server and have observed the SSL negotiation and can calculate the key used for encryption.

Because of this traffic for SSL inbound inspection does not pass over SSL proxy,

Also listen carefully around the end of this video, where they said - "you still need to allow encrypted traffic", which will be SSL -

<https://www.youtube.com/watch?v=oTivQY1RHu4>

upvoted 1 times

ashmeow 2 years ago

A makes sense. CRL is not very relevant for inbound.

upvoted 1 times

uwestani 2 years, 2 months ago

Selected Answer: D

We do inbound decryption because we do not want to allow SSL to a target server. We want to decrypt all SSL and then allow some of the decrypted apps to the target server. For decryption you do not need to allow SSL in a security policy.

We mostly use inbound decryption for Exchange and have a bunch of apps that are allowed there in the corresponding security policy. SSL we do not allow. And this works fine.

In the list of possible answers here the only one that could affect decryption and makes some kind of sense even if it may be very seldomly used, is answer D. I think it is not well written but could be some source of failure. Whereas A, B and C do not hinder inbound SSL decryption.

upvoted 1 times

  **eazy99** 2 years, 3 months ago

Selected Answer: A

I believe A is the correct answer, even if you have the certs configured correctly, if you don't have Security Policy, you can't decrypt or exclude websites from the decryption. If you google how to solve a decryption issue on PA, the first thing you get is to check your security policy. Check out this link <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CloUCAS>

upvoted 4 times

  **jonboy22** 2 years, 2 months ago



Great Answer!

upvoted 1 times

  **SMahaldar** 3 years, 1 month ago

only A

upvoted 3 times

  **Zabol** 3 years, 2 months ago

I think it is C, the question says Inbound Decryption, based on the same question in PCNSE exam Guide Certificate needs to be checked,

upvoted 2 times

  **NNgiggs** 3 years, 3 months ago

The Answer here is C, the question cannot be talking of inbound Decryption except the traffic has been allowed by the security policy. So security policy is out of question here.

Traffic that encounters any problems with decryption must have been allowed by the Security policy.

The question is talking about inbound traffic which means the firewall has imported the server certificate and its private key to be able to decrypt the traffic for inspection before passing it to the server if it is benign.

This server cert is self signed by an internal CA could be the source of the problem see answer C.

upvoted 2 times

  **rocioha** 3 years, 5 months ago

agree with answer A. you dont need tha ca. you need the server certificate imported previus to enable the ssl inb inspection


upvoted 2 times

  **achille5** 3 years, 5 months ago

Correct is A, First check the security policy then the security profiles used in the security policy that the traffic matched.

With an SSL Inbound Inspection Decryption policy enabled, the firewall decrypts all SSL traffic identified by the policy to clear text traffic and inspects it. The firewall blocks, restricts, or allows the traffic based on the Decryption profile attached to the policy and the Security policy that applies to the traffic, including and any configured Antivirus, Vulnerability Protection, Anti-Spyware, URL-Filtering, and File Blocking profiles

upvoted 1 times

  **lucaboban** 3 years, 5 months ago

Correct answer is A

Use SSL Inbound Inspection to decrypt and inspect inbound SSL traffic destined for a network server (you can perform SSL Inbound Inspection for any server if you load the server certificate onto the firewall). With an SSL Inbound Inspection Decryption policy enabled, the firewall decrypts all SSL traffic identified by the policy to clear text traffic and inspects it. The firewall blocks, restricts, or allows the traffic based on the Decryption profile attached to the policy and the Security policy that applies to the traffic, including and any configured Antivirus, Vulnerability Protection, Anti-Spyware, URL-Filtering, and File Blocking profiles. As a best practice, enable the firewall to forward decrypted SSL traffic for WildFire analysis and signature generation.

Configuring SSL Inbound Inspection includes installing the targeted server certificate on the firewall, creating an SSL Inbound Inspection Decryption policy, and applying a Decryption profile to the policy.

upvoted 1 times

  **Jpmuir** 3 years, 6 months ago

Answer is C, I do not believe it is A since a security policy is not configured to decrypt traffic. Instead a Decryption Policy must be configured.

upvoted 1 times

  **theroghert** 3 years, 6 months ago

only A

upvoted 1 times

Which two virtualization platforms officially support the deployment of Palo Alto Networks VM-Series firewalls? (Choose two.)

- A. Red Hat Enterprise Virtualization (RHEV)
- B. Kernel Virtualization Module (KVM)
- C. Boot Strap Virtualization Module (BSVM)
- D. Microsoft Hyper-V

Correct Answer: BD



Reference:

<https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series>

  **Marshpillowz** 7 months, 2 weeks ago

Answer is B and D.

<https://docs.paloaltonetworks.com/compatibility-matrix/vm-series-firewalls/vms-series-hypervisor-support>
upvoted 1 times

  **lol12** 1 year, 10 months ago

Selected Answer: BD

<https://docs.paloaltonetworks.com/compatibility-matrix/vm-series-firewalls/vms-series-hypervisor-support>
upvoted 4 times


  **Kuronekosama** 2 years ago

Selected Answer: BD

<https://docs.paloaltonetworks.com/vm-series/10-2/vm-series-deployment/license-the-vm-series-firewall/vm-series-models/vm-series-system-requirements>
upvoted 1 times

  **Dimetrodon** 1 year, 11 months ago

Did you give the exam? how many questions from here?
upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: BD

BD are correct
upvoted 1 times

  **KhalidB** 2 years, 6 months ago

B AND D ARE CORRECT
upvoted 1 times

  **SMahaldar** 3 years, 1 month ago

B and D
upvoted 2 times

  **eyelasers1** 2 years, 6 months ago

Source: <https://docs.paloaltonetworks.com/vm-series/10-1/vm-series-deployment/about-the-vm-series-firewall/vm-series-deployments.html>
upvoted 2 times

  **theroghert** 3 years, 6 months ago

B and D
upvoted 3 times

  **nk12** 4 years ago



Correct Answer: BD
upvoted 1 times



  **zhawk7661** 4 years, 1 month ago

B and D
upvoted 1 times

  **Elite4Life** 4 years, 3 months ago

docs.paloaltonetworks.com/vm-series/8-0/vm-series-deployment/about-the-vm-series-firewall/vm-series-deployments
upvoted 2 times

  **rajputparveen** 4 years, 3 months ago
<https://www.paloaltonetworks.com/prisma/vm-series>
upvoted 1 times

  **rajputparveen** 4 years, 3 months ago
B and D
upvoted 2 times

Which User-ID method maps IP addresses to usernames for users connecting through an 802.1x-enabled wireless network device that has no native integration with PAN-OS® software?

- A. XML API
- B. Port Mapping
- C. Client Probing
- D. Server Monitoring

Correct Answer: D

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/map-ip-addresses-to-users>

  **mtberdaan** Highly Voted 3 years, 2 months ago

it looks like the docs have changed and are more clear now.

XML API seems to be the right answer in this case, otherwise syslog could be possible too but that is not an answer here.

Server monitoring is not right because it assumes you are using some kind of AD server.

Answer: A

upvoted 18 times

  **mtberdaan** 3 years, 2 months ago

server monitoring description: <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/user-id-concepts/user-mapping/server-monitoring.html>

XML API description: <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/user-id-concepts/user-mapping/xml-api.html>

same for both PAN-OS 10 and 9.1 so should be relevant for the current exam

upvoted 2 times

  **SMahaldar** Highly Voted 3 years, 1 month ago

A XML API is right


upvoted 6 times

  **Bau24** Most Recent 1 month ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/user-id/user-id-concepts/user-mapping/xml-api#ide1401252-8f29-4129-9399-95673f23e772>

upvoted 1 times

  **Cro13** 3 months ago



Selected Answer: A

A is correct

In the pcnse study guide :

XML API: The PAN-OS XML API is used in cases where standard user mapping methods might not work—for example, as third-party VPNs or 802.1x-enabled wireless networks

upvoted 1 times

  **0d2fdfa** 3 months, 4 weeks ago

Selected Answer: A

This is from admin guide. It clearly says windows based agent or pan os integrated agent.

With server monitoring a User-ID agent—either a Windows-based agent running on a domain server in your network, or the PAN-OS integrated User-ID agent running on the firewall—monitors the security event logs for specified Microsoft Exchange Servers, Domain Controllers, or Novell eDirectory servers for login events.

upvoted 1 times

  **Djeep12345** 5 months, 1 week ago

The answer is A XML API, just got from PCNSE guide - The PAN-OS XML API is used in cases where standard user mapping methods might not work—for example, as third-party VPNs or 802.1x-enabled wireless networks.

upvoted 1 times



  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: A

Answer is A.

To enable an external system to send user mapping information to the PAN-OS integrated User-ID agent, create scripts that extract user login and logout events and use the events as input to the PAN-OS XML API request.

upvoted 2 times



  **JRKhan** 7 months, 4 weeks ago

Selected Answer: A

XML API

When other methods cannot be used, User-ID can consume PAN-OS XML API user login and logout messages sent from terminal servers, NAC systems, and other network devices that can format and send XML over HTTP.

upvoted 1 times

  **JRKhan** 7 months, 4 weeks ago

XML API

When other methods cannot be used, User-ID can consume PAN-OS XML API user login and logout messages sent from terminal servers, NAC systems, and other network devices that can format and send XML over HTTP.

upvoted 1 times

  **tonykolo** 8 months ago

The key phrase in the question that eliminates D is "no native integration with PAN-OS[®] software". The correct answer is A.

upvoted 1 times

  **Xuzi** 10 months ago

User-ID provides many out-of-the box methods for obtaining user mapping information. However, you might have applications or devices that capture user information but cannot natively integrate with User-ID. For example, you might have a custom, internally developed application or a device that no standard user mapping method supports. In such cases, you can use the PAN-OS XML API to create custom scripts that send the information to the PAN-OS integrated User-ID agent or directly to the firewall. The PAN-OS XML API uses standard HTTP requests to send and receive data. API calls can be made directly from command line utilities such as cURL or using any scripting or application framework that supports POST and GET requests.

upvoted 2 times

  **techplus** 11 months, 2 weeks ago

XML API, question is asking for non native way

User-ID provides many out-of-the box methods for obtaining user mapping information. However, you might have applications or devices that capture user information but cannot natively integrate with User-ID. For example, you might have a custom, internally developed application or a device that no standard user mapping method supports. In such cases, you can use the PAN-OS XML API to create custom scripts that send the information to the PAN-OS integrated User-ID agent or directly to the firewall.

upvoted 1 times

  **ANOJ1107** 11 months, 4 weeks ago

XML API

Captive Portal and the other standard user mapping methods might not work for certain types of user access. For example, the standard methods cannot add mappings of users connecting from a third-party VPN solution or users connecting to a 802.1x-enabled wireless network. For such cases, you can use the PAN-OS XML API to capture login events and send them to the PAN-OS integrated User-ID agent . See Send User Mappings to User-ID Using the XML API for details.

upvoted 1 times


  **Xuzi** 1 year ago

A - XML API

Captive Portal and the other standard user mapping methods might not work for certain types of user access. For example, the standard methods cannot add mappings of users connecting from a third-party VPN solution or users connecting to a 802.1x-enabled wireless network. For such cases, you can use the PAN-OS XML API to capture login events and send them to the PAN-OS integrated User-ID agent

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/user-id-concepts/user-mapping/xml-api>

upvoted 2 times

  **Knowledge33** 1 year, 4 months ago

Selected Answer: A



XML API is used for 802.1x implementation, according to Palo Alto. Server monitoring is not usefull on this case as the user is not connected to server.

upvoted 3 times

  **yamen123** 1 year, 4 months ago

C. Client Probing

upvoted 2 times

  **Pochex** 1 year, 6 months ago

Answer A is correct: The standard methods cannot add mappings of users connecting from a third-party VPN solution or users connecting to a 802.1x-enabled wireless network, for such cases, you can use the PAN-OS XML API, please refer to <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/user-id-concepts/user-mapping/xml-api>

upvoted 2 times

Decrypted packets from the website <https://www.microsoft.com> will appear as which application and service within the Traffic log?

- A. web-browsing and 443
- B. SSL and 80
- C. SSL and 443
- D. web-browsing and 80

Correct Answer: A

  **Pacheco** Highly Voted 4 years ago

Made an account just to tell you guys the correct answer is A.

Application is first identified as SSL on port 443, then decrypted, then identified as web-browsing on port 443. Application identification changes due to app shift, but the port number doesn't!



Correct answer is A.
upvoted 37 times

  **kerberos** 3 years, 1 month ago

you are correct!
upvoted 1 times

  **mannyvic** Highly Voted 4 years, 11 months ago

The answer should be C.... Application - HTTPS = SSL, HTTP = Web Browsing.....Service-SSL=443, Web-Browsing=80
upvoted 10 times

  **kraut** 3 years, 4 months ago

no, since ssl forward proxy is in place. ssl is getting "decrypted", and traffic is identified as web-browsing. app-id will be ssl initially but *shift*!
upvoted 3 times

  **Od2fdfa** Most Recent 3 months, 4 weeks ago


Selected Answer: A

As mentioned before, application is identified as ssl and then web browsing after decryption.
upvoted 1 times



  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: A



Answer is A.
upvoted 1 times

  **Woody** 1 year, 8 months ago

A, apparently.
upvoted 1 times

  **fireb** 2 years, 2 months ago

Option A is correct.
upvoted 1 times

  **Meko** 2 years, 2 months ago

Selected Answer: A

After being decrypted, the traffic is web-browsing traffic / port 443.
Before being decrypted, the traffic is ssl traffic / port 443.
upvoted 2 times



  **UFanat** 2 years, 2 months ago

Selected Answer: A

Correct answer: A. After a packet is decrypted we see web browsing in logs.
upvoted 2 times

  **William88** 2 years, 3 months ago

Correct answer is A
upvoted 1 times

  **datz** 2 years, 3 months ago

Selected Answer: A

If its decrypted than it will know that APP-ID = Web-Browsing and port 443 - SO A for sure
upvoted 1 times

Elvenking 2 years, 5 months ago

It is definitely "A". Just looked it up on a firewall:
show session all filter source 192.168.0.***

```
-----  
ID Application State Type Flag Src[Sport]/Zone/Proto (translated IP[Port])  
Vsys Dst[Dport]/Zone (translated IP[Port])  
-----
```

```
20714 web-browsing ACTIVE FLOW *NS 192.168.0.***[63325]/abc00/6 (**.***.***.***[35661])  
vsys1 104.208.16.90[443]/def00 (104.208.16.90[443])
```

and looking more closely:
show session id 20714

```
Session 20714  
c2s flow:  
source: 192.168.0.*** [abc00]  
dst: 104.208.16.90  
proto: 6  
sport: 63325 dport: 443  
...  
application : web-browsing  
...  
tracker stage firewall : TCP FIN  
tracker stage l7proc : proxy timer expired  
end-reason : tcp-fin  
upvoted 5 times
```

AbuHussain 2 years, 5 months ago

Selected Answer: A

Correct answer is A.
upvoted 1 times

Syn1337 2 years, 5 months ago

Selected Answer: A

Correct answer is A.
upvoted 1 times

kam1967 2 years, 10 months ago

The exam has changed. I only saw 4-5 questions from this dump on the exam.
upvoted 6 times

Breyarg 2 years, 8 months ago

ffs i just paid to use this as well..... anyone have a valid dump!?!?!? i have my exam next week :(
upvoted 1 times

LaithFraij 1 year, 6 months ago

what happened with you ?
upvoted 1 times

renzanjo 2 years, 10 months ago

Seriously??
upvoted 3 times

Bighize 2 years, 9 months ago

kam1967 is telling the truth. same thing happened to me.
upvoted 1 times

RJ45TP 2 years, 9 months ago


Have you seen a good dump anywhere else!?
upvoted 1 times

evdw 3 years, 4 months ago

Correct answer : A
upvoted 2 times

vj77 3 years, 4 months ago

Please change this answer to A
PA changed this after PAN OS 9.0
Ref:
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CmdLCAS>
upvoted 2 times

 **rocioha** 3 years, 5 months ago

A is the right answer, you can test this using any demo system of pan
upvoted 3 times

Which PAN-OS® policy must you configure to force a user to provide additional credentials before he is allowed to access an internal application that contains highly-sensitive business data?

- A. Security policy
- B. Decryption policy
- C. Authentication policy
- D. Application Override policy

Correct Answer: C

[-] **rocioha** Highly Voted 3 years, 5 months ago

C: <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/authentication-policy>

Authentication policy enables you to authenticate end users before they can access services and applications. Whenever a user requests a service or application (such as by visiting a web page), the firewall evaluates Authentication policy. Based on the matching Authentication policy rule, the firewall then prompts the user to authenticate using one or more methods (factors), such as login and password, Voice, SMS, Push, or One-time Password (OTP) authentication

upvoted 7 times

[-] **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: C

C is the correct answer.

upvoted 1 times

[-] **UFanat** 2 years, 2 months ago

Selected Answer: C

C. Authentication policy for additional credentials

upvoted 1 times

[-] **kam1967** 2 years, 10 months ago

The exam has changed. I only saw 4-5 questions from this dump on the exam. I took the exam yesterday.

upvoted 3 times

[-] **FlamingPigeon** 2 years, 8 months ago

I've taken it twice in the last month or so. Had between 20-25 questions from this dump on it.

upvoted 1 times

[-] **Elliott12** 2 years, 10 months ago

There are other people saying they took the exam just a week ago and it's most out of these dumps. Are you sure about that?

upvoted 1 times

[-] **Bighize** 2 years, 9 months ago

He's telling the truth. It happened to me to. I saw maybe 4 questions on there as well.

upvoted 1 times

[-] **secdaddy** 1 year, 11 months ago

Was true but the recent update (a couple of weeks ago) adding a few hundred more questions makes it useful again.

upvoted 2 times

[-] **theroghert** 3 years, 6 months ago

only C

upvoted 3 times

[-] **nickylake** 4 years, 1 month ago

C is the right answer

upvoted 1 times

[-] **rizky0588** 4 years, 3 months ago

Authentication Policy. (C)

upvoted 1 times

[-] **rajputparveen** 4 years, 3 months ago

C is correct

upvoted 1 times

A Security policy rule is configured with a Vulnerability Protection Profile and an action of `Deny`.

Which action will this cause configuration on the matched traffic?

- A. The configuration is invalid. The Profile Settings section will be grayed out when the Action is set to `Deny`.
- B. The configuration will allow the matched session unless a vulnerability signature is detected. The `Deny` action will supersede the per-severity defined actions defined in the associated Vulnerability Protection Profile.
- C. The configuration is invalid. It will cause the firewall to skip this Security policy rule. A warning will be displayed during a commit.
- D. The configuration is valid. It will cause the firewall to deny the matched sessions. Any configured Security Profiles have no effect if the Security policy rule action is set to `Deny`.

Correct Answer: D

Reference:

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/security-policy/security-policy-actions>

  **bbud55** Highly Voted 3 years, 5 months ago

D is correct

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/policy/security-profiles.html>

First note in above link states:

"Security profiles are not used in the match criteria of a traffic flow. The security profile is applied to scan traffic after the application or category is allowed by the security policy."

The first thing the firewall checks per it's flow is the security policy match and action. The Security Profile never gets checked if a match happens on a policy set to deny that match.

upvoted 21 times

  **Marshpillow** Most Recent 7 months, 2 weeks ago

Selected Answer: D

D is correct answer.

upvoted 1 times

  **avator** 8 months, 2 weeks ago

it is kind of burdening the firewall resource by allowing the traffic payload to be scanned once the traffic is denied to get a network service so the answer should be A or the question it self is doubting is weather the action "Deny" is it for the security rule or is it for the security profile ? if it is for the security profile it should be "Drop"

upvoted 1 times

  **Chris71Mach1** 1 year, 8 months ago

Selected Answer: D

If a traffic flow matches a security policy whose action is set to Deny, it doesn't matter what security profiles are configured within the policy, cause the traffic will be dropped regardless.

upvoted 1 times

  **Kuronekosama** 1 year, 12 months ago

Selected Answer: D

D is correct.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/security-policy/components-of-a-security-policy-rule>

Provide additional protection from threats, vulnerabilities, and data leaks. Security profiles are evaluated only for rules that have an allow action.



upvoted 1 times

  **Pakawat** 2 years, 1 month ago

D is correct : "Blocks traffic and enforces the default Deny Action defined for the application that is being denied.."

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/security-policy/security-policy-actions>

upvoted 1 times

  **Meko** 2 years, 2 months ago

Selected Answer: D

D - traffic is already deny.

upvoted 1 times

  **datz** 2 years, 3 months ago

Selected Answer: D

D for sure. if the Sec policy is already denied, no point checking Sec profiles, etc
upvoted 1 times

  **tururu1496** 2 years, 6 months ago

Selected Answer: D

Answer: D
upvoted 1 times

  **bigdaddy_69** 2 years, 7 months ago

Selected Answer: D

Allow = security profile processing.
upvoted 2 times

  **Bighize** 2 years, 9 months ago



Agreed. Failed Exam today. Only had about 8 questions from this dump. They are shifting to focus to Panaorama Deployment, Device Groups and Template stacks, UserID and mapping, Certificate questions and SSL decryption and SD-WAN. There is some Prisma on there, as well. You may not pass if you rely on this.
upvoted 3 times

  **Kane002** 2 years, 9 months ago



D. Security policies are evaluated before security profiles in the SP3. The packet will be discarded and the security profile will never be consulted.
upvoted 2 times

  **NNgiggs** 2 years, 10 months ago

A is the right answer, Vulnerability profile can only be checked if the traffic is allowed. there is no reason for a firewall to check traffic for vulnerability when it has been denied and will be dropped.
this traffic will not make it through the slow path of traffic flow in palo alto and so no session will be created because the traffic is DENIED!!!
upvoted 1 times

  **r0ze** 2 years, 10 months ago

Correct Answer: D
upvoted 1 times

  **Ceejer** 2 years, 12 months ago

Thank god for the discussion.. So many of these solutions are wrong
upvoted 1 times

  **SMahaldar** 3 years, 1 month ago

D is correct ans.
upvoted 1 times

  **Prutser2** 3 years, 2 months ago

D, the security policy is set to deny, this is enough not to allow the oacket, considering the polcy evaluation order, where security profiles get evalauted last, really the sec profile is not relevant as the packet is already denied
upvoted 1 times

A user's traffic traversing a Palo Alto Networks NGFW sometimes can reach <http://www.company.com>. At other times the session times out. The NGFW has been configured with a PBF rule that the user's traffic matches when it goes to <http://www.company.com>. How can the firewall be configured automatically disable the PBF rule if the next hop goes down?

- A. Create and add a Monitor Profile with an action of Wait Recover in the PBF rule in question.
- B. Create and add a Monitor Profile with an action of Fail Over in the PBF rule in question.
- C. Enable and configure a Link Monitoring Profile for the external interface of the firewall.
- D. Configure path monitoring for the next hop gateway on the default route in the virtual router.

Correct Answer: B

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-web-interface-help/network/network-network-profiles-monitor#>

  **UFanat** Highly Voted 2 years, 2 months ago

Selected Answer: B

B is a correct one:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/network/network-network-profiles/network-network-profiles-monitor>
A monitor profile is used to monitor IPSec tunnels and to monitor a next-hop device for policy-based forwarding (PBF) rules. In both cases, the monitor profile is used to specify an action to take when a resource (IPSec tunnel or next-hop device) becomes unavailable.
wait-recover—Wait for the tunnel to recover; do not take additional action. Packets will continue to be sent according to the PBF rule.
fail-over—Traffic will fail over to a backup path, if one is available. The firewall uses routing table lookup to determine routing for the duration of this session.

upvoted 8 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: B

Answer is B.

upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/network/network-network-profiles/network-network-profiles-monitor>
upvoted 1 times

  **kerberos** 3 years, 1 month ago



<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/policy-based-forwarding/pbf/path-monitoring-for-pbf.html>
upvoted 2 times

  **kerberos** 3 years, 1 month ago


BEHAVIOR OF A SESSION ON A MONITORING FAILURE
IF THE RULE STAYS ENABLED WHEN THE MONITORED IP ADDRESS IS UNREACHABLE
IF RULE IS DISABLED WHEN THE MONITORED IP ADDRESS IS UNREACHABLE
For an established session
wait-recover—Continue to use egress interface specified in the PBF rule
wait-recover—Continue to use egress interface specified in the PBF rule
fail-over—Use path determined by routing table (no PBF)
fail-over—Use path determined by routing table (no PBF)
For a new session
wait-recover—Use path determined by routing table (no PBF)
wait-recover—Check the remaining PBF rules. If no match, use the routing table
fail-over—Use path determined by routing table (no PBF)
fail-over—Check the remaining PBF rules. If no match, use the routing table
upvoted 1 times

  **SMahaldar** 3 years, 1 month ago

B is right
upvoted 4 times

  **rocioha** 3 years, 5 months ago

B looks correct
upvoted 2 times

  **ping_rto** 3 years, 8 months ago

B looks legit
upvoted 1 times

👤 **UmaShankar** 3 years, 10 months ago

Answer is B

upvoted 1 times

👤 **nk12** 4 years ago

Correct Answer: B

upvoted 1 times

👤 **nickylake** 4 years, 1 month ago

Monitor profile is used to specify an action to take when a resource (IPSec tunnel or next-hop device) becomes unavailable . Answer is B

upvoted 2 times

👤 **Ahmad_Zahran** 4 years, 4 months ago

B is correct.

upvoted 1 times

👤 **asmaam** 4 years, 5 months ago

correct answer is B

upvoted 1 times

👤 **shiiitboi** 4 years, 6 months ago

B is correct.

upvoted 1 times

👤 **Sammy3637** 4 years, 8 months ago

B is correct

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIFIcAK>

upvoted 2 times

👤 **tester12** 4 years, 11 months ago

Seems like the answer is B

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-web-interface-help/network/network-network-profiles-monitor#>

upvoted 2 times

What are two benefits of nested device groups in Panorama? (Choose two.)

- A. Reuse of the existing Security policy rules and objects
- B. Requires configuring both function and location for every device
- C. All device groups inherit settings from the Shared group
- D. Overwrites local firewall configuration

Correct Answer: AC

[-]  **Edu147** Highly Voted 5 years, 1 month ago

Correct ones A, C
Require something is not a benefit
upvoted 10 times

[-]  **scanossa** Most Recent 7 months, 2 weeks ago


Selected Answer: AC

Correct A and C
upvoted 1 times

[-]  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: AC

A and C are correct.
upvoted 1 times

[-]  **fireb** 2 years, 2 months ago

Correct Answers: A, C.
upvoted 1 times


[-]  **UFanat** 2 years, 2 months ago

Selected Answer: AC

A and C are correct
upvoted 3 times

[-]  **shinichi_88** 2 years, 7 months ago


A and C
upvoted 2 times

[-]  **Prutser2** 3 years, 2 months ago

a and C
upvoted 2 times

[-]  **rocioha** 3 years, 5 months ago

Correct A y C:
<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/device-groups/device-group-hierarchy>
upvoted 3 times

[-]  **lol1000** 3 years, 10 months ago

A, C is correct
upvoted 1 times

[-]  **UmaShankar** 3 years, 10 months ago

Answer is A & C
upvoted 1 times

[-]  **cthd** 4 years, 2 months ago

A and C. Creation of a device group hierarchy enables you to organize firewalls based on common policy requirements without redundant configuration. When you create objects for use in shared or device group policy once and use them many times, you reduce administrative overhead and ensure consistency across firewall policies.
upvoted 3 times

[-]  **asmaam** 4 years, 5 months ago

correct answer is A & C
upvoted 2 times

  **shiiitboi** 4 years, 6 months ago

A and C are correct. B is not a benefit.

upvoted 1 times

  **Sammy3637** 4 years, 8 months ago

Yes , A,C is correct

upvoted 3 times

Which Captive Portal mode must be configured to support MFA authentication?

- A. NTLM
- B. Redirect
- C. Single Sign-On
- D. Transparent

Correct Answer: B

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-multi-factor-authentication>

  **lol1000** Highly Voted 3 years, 10 months ago

B is correct

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/authentication/configure-multi-factor-authentication.html>

upvoted 5 times

  **Merlin0o** 1 year ago

From link:<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/authentication/configure-multi-factor-authentication>

"Configure Authentication Portal in Redirect mode to display a web form for the first authentication factor, to record authentication timestamps, and to update user mappings."

upvoted 1 times

  **Cro13** Most Recent 3 months ago

Selected Answer: B

B is correct

Step 1 : Configure Authentication Portal in Redirect mode to display a web form for the first authentication factor, to record authentication timestamps, and to update user mappings.

upvoted 1 times

  **joquin0020** 7 months, 1 week ago

Selected Answer: B

B IS CORRECT.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-ip-addresses-to-users/map-ip-addresses-to-username-using-captive-portal/captive-portal-modes>

upvoted 1 times



  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: B

B is correct.

Configure Captive Portal in Redirect mode to display a web form for the first authentication factor, to record authentication timestamps, and to update user mappings



upvoted 1 times

  **JRKhan** 7 months, 4 weeks ago

Selected Answer: B

B is correct. Captive portal is required to be configured in redirect mode for MFA to work.

upvoted 1 times

  **hpbdcB** 1 year, 11 months ago

Selected Answer: B

B as mentioned by @lol1000

upvoted 1 times

  **Trilowilly** 1 year, 10 months ago

Did you take the cert already or in process

upvoted 1 times

  **rajputparveen** 4 years, 2 months ago



B is correct

upvoted 3 times

  **_taintsmasher** 4 years, 4 months ago

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/configure-multi-factor-authentication.html>

upvoted 2 times

  **oluchi** 4 years, 5 months ago

correct

upvoted 3 times

Question #23

Topic 1

An administrator needs to implement an NGFW between their DMZ and Core network. EIGRP Routing between the two environments is required. Which interface type would support this business requirement?

- A. Virtual Wire interfaces to permit EIGRP routing to remain between the Core and DMZ
- B. Layer 3 or Aggregate Ethernet interfaces, but configuring EIGRP on subinterfaces only
- C. Tunnel interfaces to terminate EIGRP routing on an IPsec tunnel (with the GlobalProtect License to support LSVPN and EIGRP protocols)
- D. Layer 3 interfaces, but configuring EIGRP on the attached virtual router

Correct Answer: A

  **Edu147** Highly Voted  5 years, 1 month ago

Correct answer is A

Because PAN doesn't support EIGRP, therefore we need to set virtual wires

upvoted 18 times

  **GeoGR2022** Highly Voted  2 years, 3 months ago

Selected Answer: A

EIGRP is not a supported Dynamic routing protocol and Virtual Wire interfaces do not need a virtual router...



upvoted 7 times

  **Marshpillowz** Most Recent  7 months, 2 weeks ago

Selected Answer: A

Correct answer is A

upvoted 1 times

  **vj77** 3 years, 4 months ago

EIGRP is a Cisco proprietary protocol. The dynamic routing protocols supported on the PAN are RIPv2, OSPF and BGP. Answer A.

upvoted 2 times

  **UmaShankar** 3 years, 10 months ago

Answer is A

upvoted 1 times

  **alpha520** 4 years, 3 months ago

A is correct

upvoted 1 times

  **Ahmad_Zahran** 4 years, 4 months ago

Correct answer is A

Because PAN doesn't support EIGRP,

upvoted 4 times

  **asmaam** 4 years, 5 months ago

correct answer is A

upvoted 1 times

A speed/duplex negotiation mismatch is between the Palo Alto Networks management port and the switch port to which it connects. How would an administrator configure the interface to 1Gbps?

- A. set deviceconfig interface speed-duplex 1Gbps-full-duplex
- B. set deviceconfig system speed-duplex 1Gbps-duplex
- C. set deviceconfig system speed-duplex 1Gbps-full-duplex
- D. set deviceconfig Interface speed-duplex 1Gbps-half-duplex

Correct Answer: C

Reference:

<https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Change-the-Speed-and-Duplex-of-the-Management-Port/ta-p/59034>

  **Edu147** Highly Voted 5 years, 1 month ago

Correct C
I've checked in my lab

```
admin@PA-LAB-01# set deviceconfig system speed-duplex
100Mbps-full-duplex 100Mbps-full-duplex
100Mbps-half-duplex 100Mbps-half-duplex
10Mbps-full-duplex 10Mbps-full-duplex
10Mbps-half-duplex 10Mbps-half-duplex
1Gbps-full-duplex 1Gbps-full-duplex
1Gbps-half-duplex 1Gbps-half-duplex
auto-negotiate auto-negotiate
upvoted 29 times
```

  **Marshpillowz** Most Recent 7 months, 2 weeks ago



Selected Answer: C

C is the correct answer here.
upvoted 1 times

  **bearfromdownunder** 1 year, 7 months ago

Selected Answer: C

Correct answer
upvoted 1 times

  **evdw** 1 year, 8 months ago

Correct answer is C
upvoted 1 times

  **Woody** 1 year, 8 months ago



<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIMVCA0>
C
upvoted 2 times

  **Kjohnsting** 3 years, 9 months ago

Answer is B. The syntax in A is not available in the CLI.
upvoted 1 times

  **Kjohnsting** 3 years, 9 months ago

Sorry!! C is correct. Not B.
upvoted 3 times

  **lol1000** 3 years, 10 months ago

Answer is C
upvoted 1 times

  **UmaShankar** 3 years, 10 months ago

Correct is C
upvoted 1 times

  **Ahmad_Zahran** 4 years, 4 months ago

Correct C
upvoted 1 times

 **asmaam** 4 years, 5 months ago

correct answer is C

upvoted 1 times

A web server is hosted in the DMZ, and the server is configured to listen for incoming connections only on TCP port 8080. A Security policy rule allowing access from the Trust zone to the DMZ zone need to be configured to enable web browsing access to the server.

Which application and service need to be configured to allow only cleartext web-browsing traffic to this server on tcp/8080?

- A. application: web-browsing; service: application-default
- B. application: web-browsing; service: service-https
- C. application: ssl; service: any
- D. application: web-browsing; service: (custom with destination TCP port 8080)

Correct Answer: D

  **nhema** Highly Voted 3 years, 5 months ago

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/app-id-features/app-default-strict.html>

Application default for web-browsing is port 80

upvoted 8 times

  **eyelasers1** 2 years, 6 months ago

Also can be referenced based on web-browsing info from <https://applipedia.paloaltonetworks.com/>

upvoted 1 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: D

Correct answer is D

upvoted 1 times

  **nguyendtv50** 1 year, 3 months ago

The correct answer is: Application: web-browsing Service: application-default Explanation: Since the server is listening on TCP port 8080, we need to use a custom service to specify this port. However, the question specifically asks for allowing only clear-text web-browsing traffic, which means HTTP traffic on port 8080. The 'web-browsing' application represents HTTP traffic, and the 'application-default' service includes TCP ports commonly used for HTTP traffic, including port 8080. Therefore, the correct configuration is to use the 'web-browsing' application and the 'application-default' service.



upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: D



need to create a rule with custom service for port 8080 and application web-browsing

upvoted 1 times

  **ToddJ** 2 years, 4 months ago



oops, B says https, so no, it is not correct

upvoted 1 times

  **ToddJ** 2 years, 4 months ago

B is correct, service-http has a setting of 80 and 8080

upvoted 1 times

  **GeoGR2022** 2 years, 3 months ago



but the B question talks about service-https which has a setting of port 443/tcp

upvoted 1 times

  **tururu1496** 2 years, 6 months ago

This depends on the Dst NAT configuration. Could be A, but is likely D

upvoted 1 times

  **ev333** 2 years, 6 months ago

Selected Answer: D

D is correct

upvoted 4 times

  **Jared28** 2 years, 6 months ago


D - Where I think this question is trying to mislead you is the *Services* object, not the web-browsing app, is tcp/80 and tcp/8080

upvoted 1 times



  **RamanJoshi** 2 years, 7 months ago

Selected Answer: D



D is correct
upvoted 2 times

  **Igkhan** 2 years, 9 months ago

D is correct!
upvoted 2 times

  **rgbykkk** 2 years, 10 months ago



Can we not change the answers based upon the discussion?
upvoted 1 times

  **FS68** 2 years, 11 months ago



D is correct
upvoted 3 times

  **Guigo** 3 years ago

Answer is D for sure.
upvoted 2 times

  **YasserSaied** 3 years, 2 months ago

D -- couldn't be anything else
upvoted 1 times

  **evdw** 3 years, 4 months ago

Correct answer: D
upvoted 2 times

  **aadach** 3 years, 5 months ago

only D
upvoted 3 times

If the firewall has the following link monitoring configuration, what will cause a failover?

The screenshot shows the Palo Alto Networks configuration interface for Link Monitoring. The 'Link Monitoring' section is enabled with a failure condition of 'all'. A 'Link Group' named 'Link_group' is configured with 'all' as the group failure condition and includes interfaces 'ethernet1/3' and 'ethernet1/6'.

Name	Enabled	Group Failure Condition	Interfaces
Link_group	<input checked="" type="checkbox"/>	all	ethernet1/3 ethernet1/6

- A. ethernet1/3 and ethernet1/6 going down
- B. ethernet1/3 going down
- C. ethernet1/3 or ethernet1/6 going down
- D. ethernet1/6 going down

Correct Answer: A

rocioha Highly Voted 3 years, 5 months ago

A is the right answer because the question refers to all not any.

upvoted 11 times

Marshpillowz Most Recent 7 months, 2 weeks ago

Selected Answer: A

Correct answer is A

upvoted 1 times

aatechler 1 year, 10 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/high-availability/ha-concepts/failover>

upvoted 3 times

UFanat 2 years, 2 months ago

Selected Answer: A

Failure condition - ALL. It means both interfaces should go down.

upvoted 3 times

tururu1496 2 years, 6 months ago

Selected Answer: A

Answer: A

upvoted 2 times

homersimpson 2 years, 8 months ago

A is correct because the "Group Failure Condition" in the image is "all". If it said "any", then losing link on either interface would cause failover.

upvoted 4 times

In the image, what caused the commit warning?

The screenshot shows the Palo Alto Networks GUI. The 'Device Certificates' tab is active, displaying a table with two certificates:

Name	Subject	Issuer	CA	K...	Expires	Sta...	Al...	Usage
FWDtrust	CN = FWDtrust	DC = local, DC = lab, CN = lab-SRV2016-LABCA-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 29 02:02:05 2020 GMT	valid	RSA	Forward Trust Certificate
FWD-UnTrust	CN = FWD-UnTrust	CN = FWD-UnTrust	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 29 02:06:36 2019 GMT	valid	RSA	Forward Untrust Certificate

A 'Commit Status' dialog box is open, showing the following details:

- Operation: Commit
- Status: Completed
- Result: Successful
- Details: Configuration committed successfully
- Warnings: Warning: cannot find complete certificate chain for certificate FWDtrust (Module: device)

- A. The CA certificate for FWDtrust has not been imported into the firewall.
- B. The FWDtrust certificate has not been flagged as Trusted Root CA.
- C. SSL Forward Proxy requires a public certificate to be imported into the firewall.
- D. The FWDtrust certificate does not have a certificate chain.

Correct Answer: A

Reference:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/troubleshoot-and-monitor-decryption/decryption-logs/repair-incomplete-certificate-chains>

AdamLolzSmith Highly Voted 3 years, 3 months ago

Option A. The FWDtrust is a CA certificate type capable of signing other certificates.

That means either it's a Root Certificate or Intermediate certificate. If it was a Root Certificate, then you wouldn't get that warning. That means the certificate is an intermediate and you need to import its Root Certificate.

upvoted 18 times

Prutser2 3 years, 2 months ago

correct, in addition, the CA for FWDtrust is some LAB CA, says it under issuer, so definitely not root

upvoted 2 times

hcir Most Recent 2 months, 3 weeks ago

D is the answer. It is a simple warning that states that there is no chain

upvoted 1 times

JRKhan 7 months, 4 weeks ago

Selected Answer: A

Under issuer, it tells us which root CA signed the FWDTrust certificate. Correct answer is A. FWDTrust needs to be a CA (intermediate in this case) in order for it to be able to sign the server certs so that clients accessing an external server or website can tell if the firewall trusts those server certs or not.

upvoted 1 times

Micutzu 10 months, 3 weeks ago

Selected Answer: B

I think the correct answer is B.

upvoted 1 times

Micutzu 10 months, 3 weeks ago

I think the correct answer is B.

upvoted 1 times

455_qq 2 years, 1 month ago

Option A.



upvoted 1 times

  **Jared28** 2 years, 5 months ago

Selected Answer: A

A - Tested in lab

upvoted 3 times

  **unknid** 2 years, 7 months ago

Selected Answer: A

A. because FWDtrust has a chain but it's not present in the firewall.

upvoted 1 times

  **Kane002** 2 years, 9 months ago

D. The problem, as it says itself, is that it does not have a complete chain of trust. The solution would be to add in any intermediate CAs that the NGFW doesn't have as root CAs to restore the chain, but the problem is the chain.

upvoted 2 times

  **myname_1** 1 year, 8 months ago

D is ambiguous. D is saying that there is no certificate chain for that cert, but there is because the issuer for the FWDTrust is not the same CN as the subject of FWDTrust

upvoted 1 times

  **Biz90** 2 years, 10 months ago

Hi Team to add It is A as other users have done I tested this as well.



If you're using an External/Internal PK, you need to ensure to import the Root CA, in which once you create, generate your CSR, and reimport the Trust cert into the Firewall. The Trust cert should fall into the COC. If this was a self-signed cert (as I have also labbed) you can simple have that on the FW without a COC.

upvoted 2 times

  **FS68** 2 years, 11 months ago

A. because FWDtrust has a chain but it's not present in the firewall.

upvoted 2 times

  **bluejl** 3 years, 2 months ago



A. Tested in lab.

upvoted 3 times

  **Joey456** 3 years, 4 months ago

A: <https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/troubleshoot-and-monitor-decryption/decryption-logs/repair-incomplete-certificate-chains.html>

upvoted 2 times

  **evdw** 3 years, 4 months ago

I think answer is A : is not self-signed-certificate -> so other certificate signed this certificate, if that is not imported there is no chain of trust

upvoted 2 times

  **trashboat** 3 years, 4 months ago

The answer is D. When importing a CA certificate, the full certificate chain must be present in the certificate information for proper identification/verification.

A can't be true because the certificate in question is imported is a CA cert.

B can't be true because the certificate in question is imported as a trusted root CA.

C can't be true because SSL Forward proxy can be set up using self-signed certs.

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/configure-ssl-forward-proxy.html>

upvoted 4 times

  **kerberos** 2 years, 10 months ago

correct!

upvoted 1 times

  **homersimpson** 2 years, 8 months ago



Agreed

upvoted 1 times

  **myname_1** 1 year, 8 months ago

The certificate in the screenshot is a CA, because it has to be a CA for forward trust. The issue is that FWDTrust's (Which is CN = "Lab-SRV2016...") does not have its CA imported. If it were the CA of its chain, the subject would match the issuer.

upvoted 1 times

  **Qintao** 3 years, 4 months ago

A is inaccurate, no need to be a Trust root CA

upvoted 2 times

  **Paul_great** 3 years, 5 months ago

The answer is A. The issuer of the cert was not imported in the firewall and the firewall could not build a chain because of it.

upvoted 1 times

Question #28

Topic 1

Which method does an administrator use to integrate all non-native MFA platforms in PAN-OS® software?

- A. Okta
- B. DUO
- C. RADIUS
- D. PingID

Correct Answer: C

  **mmed** Highly Voted 3 years, 5 months ago

C

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/authentication-types/multi-factor-authentication>

The firewall makes it easy to implement MFA in your network by integrating directly with several MFA platforms (Duo v2, Okta Adaptive, PingID, and Okta Adaptive) and integrating through RADIUS with all other MFA platforms.

upvoted 8 times

  **eyelasers1** 2 years, 6 months ago

Still correct. Updated URL: <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/authentication/authentication-types/multi-factor-authentication.html>

upvoted 1 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: C

Answer is C

upvoted 1 times

  **Merlin0o** 1 year ago

Selected Answer: C

C Still valid:

<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/authentication/configure-multi-factor-authentication>

upvoted 1 times

  **Questionario** 1 year, 5 months ago

guess with newer versions it would be SAML?

upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: C


Okta, Duo and PingID are already native integrations. RADIUS allows you to integrate with other MFA platforms

upvoted 3 times

  **Prutser2** 3 years, 2 months ago

pan OS 8.1 uses RADIUS for MFA with MS authenticator in Azure, FYI

upvoted 2 times

  **johnsonwale** 3 years, 3 months ago

C

<https://www.examttopics.com/exams/palo-alto-networks/pcnse/view/7/>

upvoted 2 times

How would an administrator monitor/capture traffic on the management interface of the Palo Alto Networks NGFW?

- A. Use the debug dataplane packet-diag set capture stage firewall file command.
- B. Enable all four stages of traffic capture (TX, RX, DROP, Firewall).
- C. Use the debug dataplane packet-diag set capture stage management file command.
- D. Use the tcpdump command.

Correct Answer: D

Reference:

<https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Run-a-Packet-Capture/ta-p/62390>

  **jairusster** Highly Voted 5 years, 4 months ago

Correct answer is D. Use TCP Dump: <https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/monitoring/take-a-packet-capture-on-the-management-interface>
upvoted 21 times

  **eyelasers1** 2 years, 6 months ago



From <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/take-packet-captures/take-a-packet-capture-on-the-management-interface.html>

"The tcpdump CLI command enables you to capture packets that traverse the management interface (MGT) on a Palo Alto Networks firewall."
upvoted 1 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: D

Correct answer is D
upvoted 1 times


  **Woody** 1 year, 8 months ago

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/take-packet-captures/take-a-packet-capture-on-the-management-interface>
Vote for D.
upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: D



Correct answer is D
upvoted 3 times

  **ochc** 3 years, 9 months ago

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/take-packet-captures/take-a-packet-capture-on-the-management-interface.html>
upvoted 1 times

  **yashishinde** 4 years, 2 months ago

The tcpdump CLI command enables you to capture packets that traverse the management interface (MGT) on a Palo Alto Networks firewall. ans:d
upvoted 2 times

  **Ripu** 4 years, 2 months ago



Answer :D
upvoted 2 times

  **Ahmad_Zahran** 4 years, 4 months ago

Correct answer is D.
upvoted 2 times

  **asmaam** 4 years, 5 months ago

correct answer is D
upvoted 1 times

  **khalmrj** 4 years, 6 months ago

Correct answer is D
upvoted 2 times

An administrator needs to optimize traffic to prefer business-critical applications over non-critical applications. QoS natively integrates with which feature to provide service quality?

- A. Port Inspection
- B. Certificate revocation
- C. Content-ID
- D. App-ID

Correct Answer: D

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/quality-of-service/qos-concepts/qos-for-applications-and-users#idaed4e749-80b4-4641-a37c-c741aba562e9>



  **Prutser2** Highly Voted  3 years, 2 months ago

D, QoS marking can be done on a security policy, so marking can be done based on app_ID
upvoted 5 times



  **Marshpillowz** Most Recent  7 months, 2 weeks ago

Selected Answer: D

Correct answer is D
upvoted 1 times

  **JakeN** 1 year, 6 months ago

App ID naturally
upvoted 1 times

  **hpbdc** 1 year, 11 months ago

Selected Answer: D

D as mentioned by the others
upvoted 1 times

  **yashishinde** 4 years, 2 months ago

asn :D-The Palo Alto Networks firewall provides this capability by integrating the features App-ID and User-ID with the QoS configuration
upvoted 2 times

  **rizky0588** 4 years, 3 months ago

The answer is D
upvoted 3 times

A session in the Traffic log is reporting the application as `incomplete.`

What does `incomplete` mean?


- A. The three-way TCP handshake was observed, but the application could not be identified.
- B. The three-way TCP handshake did not complete.
- C. The traffic is coming across UDP, and the application could not be identified.
- D. Data was received but was instantly discarded because of a Deny policy was applied before App-ID could be applied.

Correct Answer: B

  **west33637** Highly Voted  1 year, 10 months ago

Selected Answer: B

answer is B - <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC>
upvoted 5 times

  **Marshpillowz** Most Recent  7 months, 2 weeks ago

Selected Answer: B

B is correct

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC>
upvoted 1 times

  **Frightened_Acrobat** 1 year, 1 month ago

Selected Answer: B

I thought it could be A at first, but reading PaloSteve's comment, it looks like A has the wrong language. "Observed" rather than "complete" and left out "not enough data."

upvoted 1 times

  **PaloSteve** 1 year, 1 month ago

The answer looks to be A or B, if the article is still valid. It was last modified 2 years ago.

From the article (<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC>): Incomplete means that either the three-way TCP handshake did not complete OR the three-way TCP handshake did complete but there was no enough data after the handshake to identify the application.

Insufficient data means not enough data to identify the application.

Unknown-tcp means the firewall captured the three-way TCP handshake, but the application was not identified.

Not-applicable means that the Palo Alto device has received data that will be discarded because the port or service that the traffic is coming in on is not allowed, or there is no rule or policy allowing that port or service.

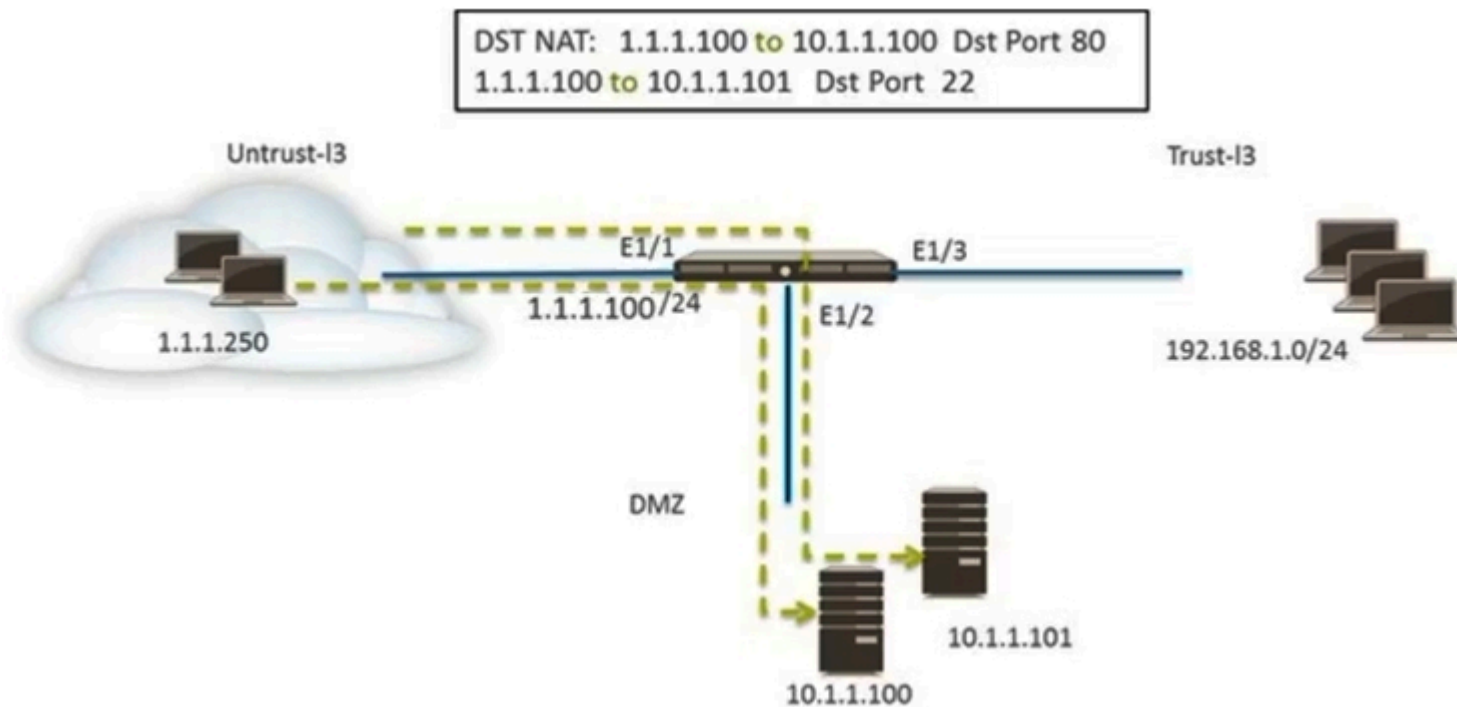
upvoted 4 times

  **yazid0016** 1 year, 8 months ago

Answer is B

upvoted 3 times

Refer to the exhibit.



An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host

A (10.1.1.100) receives HTTP traffic and Host B (10.1.1.101) receives SSH traffic.

Which two Security policy rules will accomplish this configuration? (Choose two.)

- A. Untrust (Any) to Untrust (10.1.1.1), web-browsing $\lambda\epsilon$ " Allow
- B. Untrust (Any) to Untrust (10.1.1.1), ssh $\lambda\epsilon$ " Allow
- C. Untrust (Any) to DMZ (1.1.1.100), web-browsing $\lambda\epsilon$ " Allow
- D. Untrust (Any) to DMZ (1.1.1.100), ssh $\lambda\epsilon$ " Allow
- E. Untrust (Any) to DMZ (10.1.1.100, 10.1.1.101), ssh, web-browsing $\lambda\epsilon$ " Allow

Correct Answer: CD

- achille5** Highly Voted 3 years, 5 months ago
 C, D and D should be Untrust (Any) to DMZ (1.1.1.101), ssh - Allow
 upvoted 6 times
- anak1n** 3 years, 5 months ago
 yeah the answer .101 last octet is wrong but is straight forward ;)
 upvoted 1 times
- achille5** 3 years, 4 months ago
 Correction: It's CD. NAT policy is given already. Ignore Above :D
 upvoted 2 times
- utahman3431** 3 years, 5 months ago
 I think it is correct as written. 1.1.1.100 is the pre-NAT IP, and all web/ssh traffic should go to it. Once it hits the NAT policy then the IP will be translated to 10.1.1.100/10.1.1.101
 upvoted 6 times
- confusion** Highly Voted 2 years, 6 months ago
Selected Answer: CD
 Security policies use pre-NAT addresses and post-NAT zones. so C+D
 upvoted 5 times
- Marshpillowz** Most Recent 7 months, 2 weeks ago
Selected Answer: CD
 Answer is C and D
 upvoted 1 times
- JRKhan** 7 months, 4 weeks ago
Selected Answer: CD
 C and D are correct. Security policies use post-nat zones and pre-nat ip addresses.



upvoted 1 times

  **_3_** 9 months, 3 weeks ago

Selected Answer: E

Wouldn't E be the only possible answer? Someone correct me if I am wrong but security policies are applied post-NAT, so C and D referencing the pre-NAT IP would be incorrect. E is the only answer with correct post-NAT zone and IPs.

upvoted 2 times

  **nsg79** 11 months, 2 weeks ago

Selected Answer: AB

correct answer is AB

answer is right here from palo alto:


<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/nat/nat-configuration-examples/destination-nat-exampleone-to-many-mapping#idfe075fbd-c132-4c52-b4c4-5adc7f4fc0bc>

upvoted 2 times

  **Kris92** 10 months ago

The link explains this exact scenario and if you look at the security policy from the documentation it matches C, D. You might have looked at the NAT policy which needs to be configured with source and destination zone Untrust, but the question is about the security policy.

upvoted 2 times

  **Redrum702** 1 year, 2 months ago

Ok, I understood this was to write a DNAT policy. Correct answers are C/D. But for a DNAT it would be A/B :)

upvoted 1 times

  **Redrum702** 1 year, 2 months ago

A/B: For the destination IP address to be translated, a destination NAT rule from zone Untrust-L3 to zone Untrust-L3. DNAT allows you to rewrite the destination IP address and port of incoming traffic and redirecting it to a different destination IP address and port. DNAT is commonly used for scenarios such as exposing internal servers to the internet or redirecting traffic to specific services.



<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/nat/nat-configuration-examples/destination-nat-exampleone-to-one-mapping>

upvoted 1 times

  **daytonadave2011** 1 year, 5 months ago

This is a very poorly written question with answers. It should say D. 10.1.1.101 instead of 10.1.1.100.



upvoted 2 times

  **lol12** 1 year, 10 months ago

Selected Answer: CD

Answer CD

upvoted 1 times

  **fireb** 1 year, 10 months ago

Correct answers: C & D.

upvoted 1 times

  **secdaddy** 1 year, 11 months ago

Selected Answer: CD

Agree C and D assuming a typo in D (otherwise maybe CE)

The box at the top is misleading since the NAT rules must use the pre-nat IP 1.1.1.100 as dest

actual DNAT rules must refer to pre-translated dest address 1.1.1.100 with szone and dzone both = untrust-l3

security rules also use pre-translated dest address 1.1.1.100 and szone untrust-l3 but dzone = DMZ

upvoted 1 times

  **juan_L** 2 years ago

Shame- I hope to be a typo and actually D - refers to 1.1.1.101, E - means that it opens ssh for the rest of the company, OK maybe cant access from internet but now it have created a ssh open for all the zones of the company where NAT is not quered, this is a very, very, very bad example. Try not to learn from that questions.

Sadly if there is no typo, correct is CE

upvoted 1 times

  **Pretorian** 2 years ago

Why the entire company? there are only 2 IP's as destination.

upvoted 1 times

  **Pretorian** 2 years ago

Plus destination is DMZ only.

upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: CD

For firewall rules you should use DMZ zone but external IP. For NAT rules - External (untrust) zone and external IP.

upvoted 2 times

  **Kane002** 2 years, 9 months ago

I actually got this exact question on my PCNSA.
upvoted 1 times

  **Prutser2** 3 years, 2 months ago

security policies use pre-NAT addresses, but post NAT zones. so D
upvoted 1 times

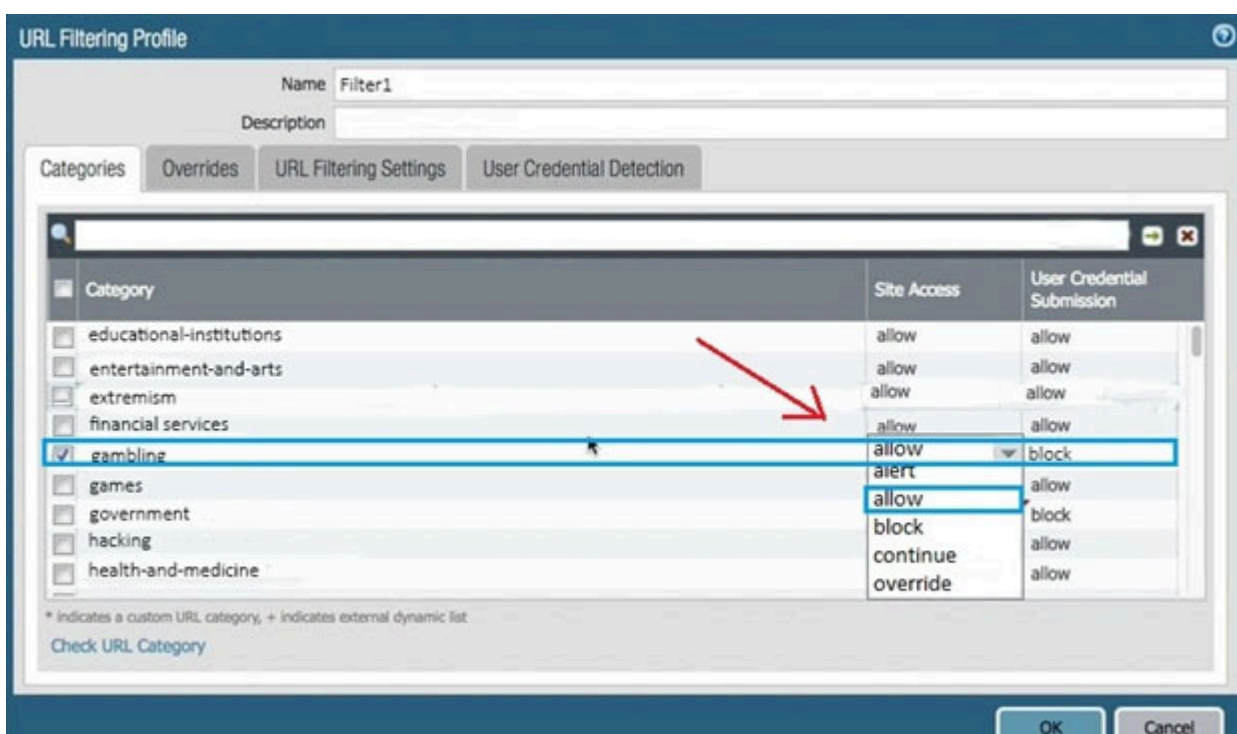
An administrator needs to determine why users on the trust zone cannot reach certain websites. The only information available is shown on the following image.

Which configuration change should the administrator make?

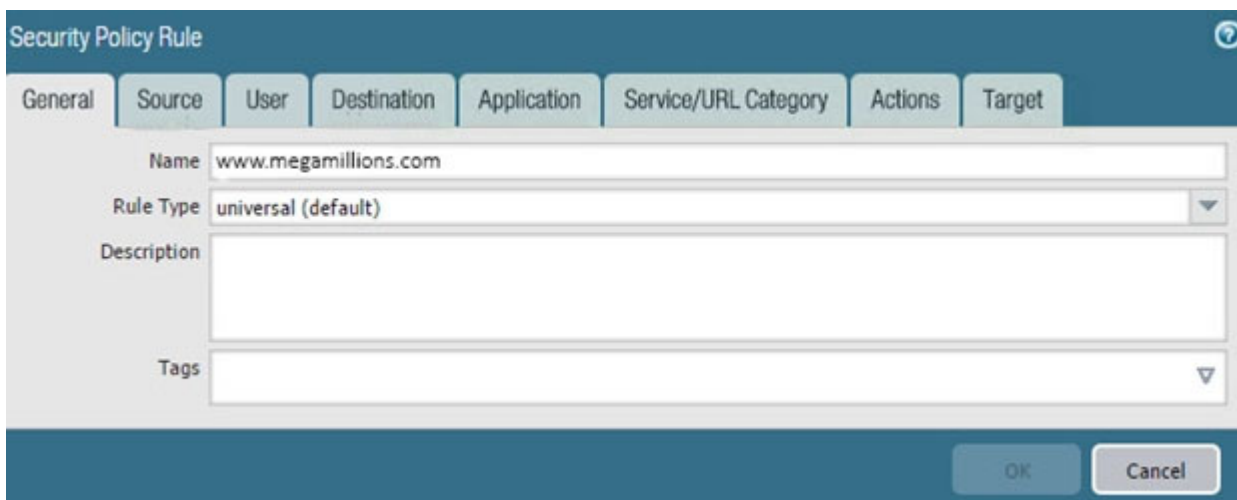
A.



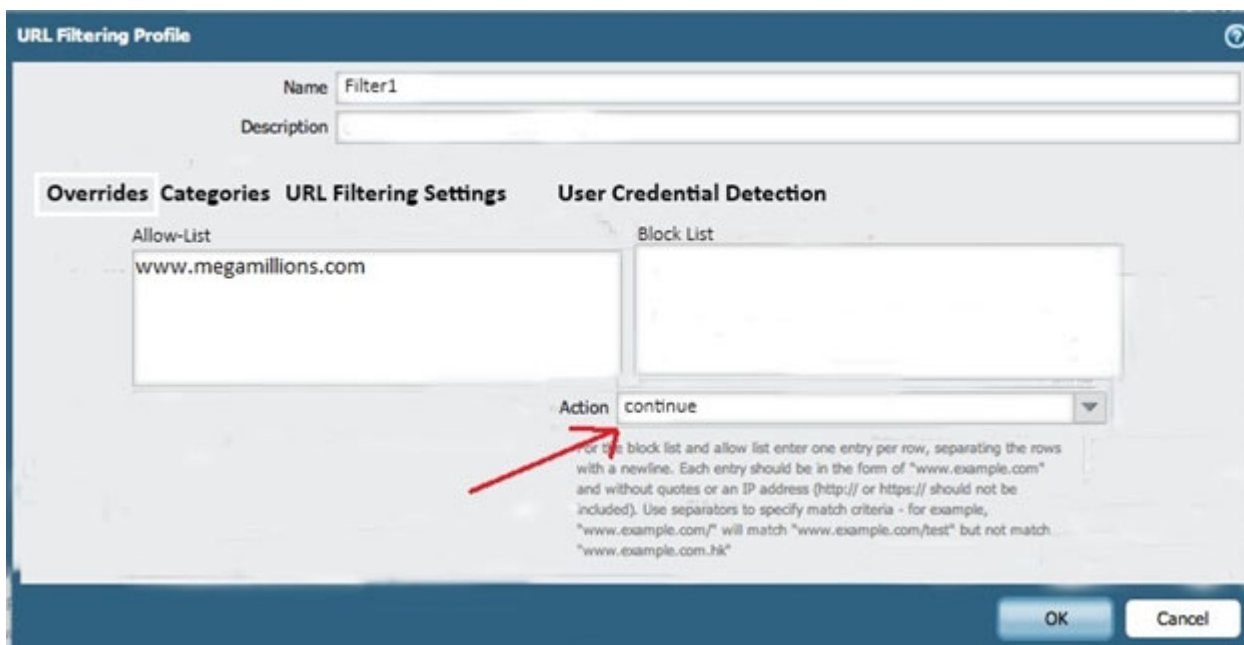
B.



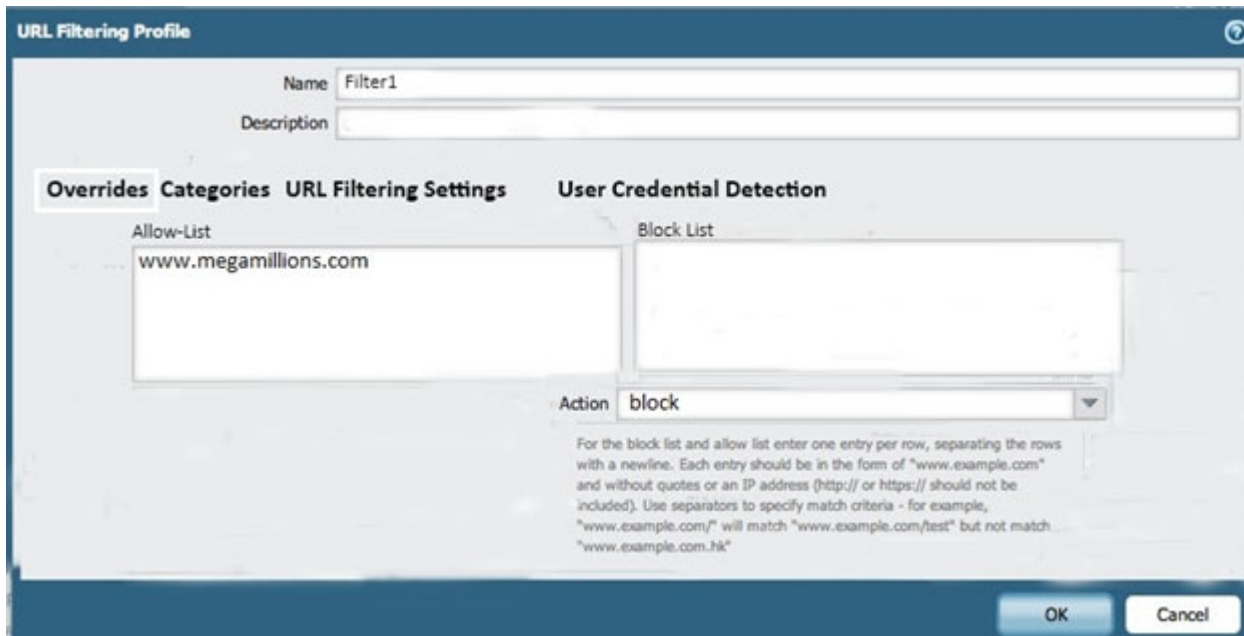
C.



D.



E.



Correct Answer: B

- frodo1791** Highly Voted 3 years, 4 months ago
 B is correct... the question is talking about "certain websites", options D and E are talking about just one specific website.
 upvoted 11 times
- 428cd48** Most Recent 5 months, 3 weeks ago
 Horribly formulated question. Confusing.
 upvoted 3 times
- Marshpillowz** 7 months, 2 weeks ago
 B is correct
 upvoted 1 times
- Pochex** 1 year, 6 months ago
 Answer B would be the best option since it is allowing 'gambling'.

Answer A is part of a session id, there is no way to configure it.
 Answer C refers to the policy name, and should not affect anything.
 Answers D and E display config no longer available in PANOS 9.0 and higher

I don't believe this question would be included in the current PCNSE exam.
 upvoted 3 times
- Frightened_Acrobat** 1 year, 6 months ago
 All of these answers are wrong. This question was for PAN-OS before 9.0.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000008UtaCAE&lang=en_US%E2%80%A9
 In PAN-OS 9, and above, this is how to add a URL exception:
 To configure exceptions to URL categories, you can create a custom URL category (GUI: Objects > Custom Objects > URL Category).
 This question in no way should be on the exam, but if it was, B could be the only viable solution.
 upvoted 2 times
- lol12** 1 year, 10 months ago
 Should be A. First screenshot Log View with the issue. Second screenshot should be labelled as A
 upvoted 2 times
- Chris71Mach1** 1 year, 8 months ago
 A log view isn't a configuration change. (A) is unfortunately the most incorrect answer available.
 upvoted 3 times

[-]  **DriVen** 2 years, 1 month ago


IN addition, the logic here is bizzare...the question asks "An administrator needs to determine why"...THIS has already been determined..why? Well obviously, because it's a blocked category, so logically speaking there is no right answer here

upvoted 1 times

[-]  **DriVen** 2 years, 1 month ago


Another super dumb question...of course you need to allow gambling for all your employees, I mean why not... xD

upvoted 2 times

[-]  **datz** 2 years, 3 months ago

ITS B, certain websites/Category needs to be whitelisted. They want to Gamble. Let them Gamble lol

upvoted 4 times

[-]  **Biz90** 2 years, 10 months ago


I believe this is B based on the block action for the credentials. As this will block a user if they are required to use credentials to access a page for example a login/webform etc.

upvoted 1 times

[-]  **Narendragpt** 3 years, 5 months ago

Answer is B . The question is asking certain websites are not accessible so only B is correct option to fulfill the requirement here .

upvoted 1 times

[-]  **nhema** 3 years, 5 months ago

First of all, A should be the exhibit... besides that:

B will allow the whole gambling category

upvoted 2 times

[-]  **anak1n** 3 years, 5 months ago


so then it should be D not A, A is just showing the log itself, B indeed it will allow the whole gambling that's why in URL filtering you will set this website to CONTINUE not Block

upvoted 1 times

[-]  **petersummer** 3 years, 5 months ago

It's mentioned certain sites, so B will allow all whole category of sites, not only one that is shown on D. B is correct

upvoted 3 times

[-]  **rocioha** 3 years, 5 months ago

I think is E, because of the block option

upvoted 2 times

Which three settings are defined within the Templates object of Panorama? (Choose three.)

- A. Setup
- B. Virtual Routers
- C. Interfaces
- D. Security
- E. Application Override

Correct Answer: ABC

— **Edu147** Highly Voted 5 years, 1 month ago

Correct A,B,C
D and E are Device Group Objects
upvoted 19 times

— **rocioha** Highly Voted 3 years, 5 months ago

Template: network and device. Device Groups= Object and Policies
upvoted 9 times

— **scanossa** Most Recent 7 months, 2 weeks ago

Selected Answer: ABC

Templates involves Devices and Network settings
upvoted 1 times

— **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: ABC

A, B, C are correct
upvoted 1 times

— **JRKhan** 7 months, 4 weeks ago

Selected Answer: ABC

Panorama templates allow to configure Device (Setup) and Network (Interfaces & Virtual Routers) settings on the managed firewalls.
upvoted 2 times

— **UFanat** 2 years, 2 months ago

Selected Answer: ABC

Correct A,B,C
D and E are Device Group Objects
upvoted 2 times

— **fireb** 2 years, 3 months ago

Correct options: A, B, C.
upvoted 1 times

— **kambata** 3 years, 10 months ago

A, B, C
upvoted 1 times

— **guilherme_a** 3 years, 11 months ago

A B and C
upvoted 1 times

— **hyperv89** 4 years ago

A - B - C .
upvoted 1 times

— **Ripu** 4 years, 2 months ago

Answer:A,B,C it is correct answer
upvoted 3 times

— **AMARSIL** 4 years, 3 months ago

Correct A,B,C
upvoted 2 times

 **asmaam** 4 years, 5 months ago

correct answer are ABC

upvoted 3 times

A customer has an application that is being identified as unknown-tcp for one of their custom PostgreSQL database connections. Which two configuration options can be used to correctly categorize their custom database application? (Choose two.)

- A. Application Override policy.
- B. Security policy to identify the custom application.
- C. Custom application.
- D. Custom Service object.

Correct Answer: AC

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clc6CAC>



  **dhanala** Highly Voted 4 years, 2 months ago

B and C is correct, if we are choosing C custom application then in the security policy we need to choose Custom Application.
upvoted 21 times

  **GivemeMoney** 2 years, 7 months ago

Yep, B and C



<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/app-id/manage-custom-or-unknown-applications.html>
upvoted 4 times

  **Gabbranch** 9 months, 2 weeks ago

Disagree - Question is how to correctly categorize the applicaiton.

Security Policy is how to deal with an unknown app - as in how to allow it despite having no app-id for it. It does not deal with categorizing the app.

upvoted 1 times

  **datz** 2 years, 3 months ago

B. Security policy to identify the custom application.

B is there to identify customer app-ID? as advised it is custom so allowing traffic is not issue to find out what APP-ID is inside a Traffic

Must be A and C

upvoted 2 times

  **tester12** Highly Voted 4 years, 11 months ago

Answer is A and C
upvoted 10 times

  **eaakgul** Most Recent 3 months, 1 week ago



Correct answer is A & C
upvoted 1 times

  **1f2c588** 3 months, 3 weeks ago

A&C are correct.

Application Override to baypass the App-ID and the custom application to indentifie the applications, (then the tow actions to catigorize the applicaitonà)

upvoted 1 times

  **0d2fdfa** 3 months, 4 weeks ago

Selected Answer: AC

Which two configuration options can be used to correctly categorize

It is about categorization and not the implementation.



upvoted 1 times

  **gradski** 5 months ago

Selected Answer: BC

<https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/app-id/manage-custom-or-unknown-applications>

upvoted 2 times

  **428cd48** 5 months, 2 weeks ago

on 3/22 exam

upvoted 1 times

[-]  **Mar_a_Lagoon** 5 months, 3 weeks ago

Selected Answer: AC

AC, refer to the other replies. Security policy will never id anything
upvoted 1 times

[-]  **SH_** 6 months, 4 weeks ago

Selected Answer: AC

security policy doesn't identify apps, app-id does.

create a custom app AND/OR use an app override policy to identify the app based on traffic using it. THEN consult the security policy to figure out whether to block or allow the traffic.


upvoted 1 times

[-]  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: AC

A, C correct answer here

upvoted 1 times

[-]  **JRKhan** 7 months, 4 weeks ago

Selected Answer: AC

A & C are correct. Security policy allows or denies the traffic, doesnt categorise the application. The two ways you can categorise an application is to define a custom App or use Application override policy where you will still need to define the application ports, IP addresses, zones etc. to identify the application. Application override is not recommended however and should only be used as a temporary workaround while the work is going on to define a custom app for the same traffic.

upvoted 2 times

[-]  **onkel_andi** 9 months ago

Selected Answer: AC

A and C correct

upvoted 2 times

[-]  **dorf05** 9 months ago

Selected Answer: BC

I think 'A' is wrong because..For internal applications and applications for which there is no App-ID, create custom applications to gain layer 7 visibility into traffic. Don't use Application Override policy because it bypasses layer 7 processing and threat inspection. The use cases for Application Override are unusual situations with SMB or SIP traffic.

upvoted 1 times


[-]  **Nina93523** 9 months, 1 week ago

Selected Answer: BC

-Manage Custom or Unknown Applications

Create a Custom Application with a signature and attach it to a security policy, or create a custom application and define a custom timeout. Avoid creating Application Override

upvoted 1 times

[-]  **gc999** 9 months, 2 weeks ago

Selected Answer: BC

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/manage-custom-or-unknown-applications#:~:text=Create%20a%20Custom%20Application%20with%20a%20signature%20and%20attach%20it%20to%20a%20security%20policy%2C%20or%20create%20a%20custom%20application%20and%20define%20a%20custom%20timeout.%20Avoid%20creating%20Application%20Override>

upvoted 2 times

[-]  **skullomania** 9 months, 3 weeks ago

Selected Answer: AC

Stop inventing people. You don't create a security policy to identify the custom application. Correct options are A and C. I'm a PCNSE engineer since 2017 and PCNSC since 2019.

upvoted 3 times

[-]  **Xuzi** 10 months ago

The following choices are available to handle unknown applications:

Create security policies to control unknown applications by unknown TCP, unknown UDP or by a combination of source zone, destination zone, and IP addresses.

Create a Custom Application with a signature and attach it to a security policy, or create a custom application and define a custom timeout. Avoid creating Application Override policies because they bypass layer 7 application processing and threat inspection, and use less secure stateful layer 4 inspection instead. Instead, use custom timeouts so that you can control and inspect the application traffic at layer 7.

upvoted 1 times

An administrator logs in to the Palo Alto Networks NGFW and reports that the WebUI is missing the Policies tab.
Which profile is the cause of the missing Policies tab?



- A. Admin Role
- B. WebUI
- C. Authentication
- D. Authorization

Correct Answer: A

  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: A

Correct answer is A
upvoted 1 times

  **hpbdc** 1 year, 11 months ago

Selected Answer: A

voting comment for option A
upvoted 2 times


  **JMIB** 2 years ago

Option A is correct.
upvoted 1 times

  **Pretorian** 2 years, 1 month ago

Typical malicious PANW test question using obscure terms. What does the word "Profile" have to do with anything here? The answer is "Admin Role"...

upvoted 3 times

  **fireb** 2 years, 2 months ago

Option A is correct.
upvoted 1 times

  **rocioha** 3 years, 4 months ago

a is the correct answer because it depends of the admin role assigned
upvoted 4 times

  **kumanan** 3 years, 4 months ago



Answer: A
upvoted 4 times

An administrator has left a firewall to use the default port for all management services.

Which three functions are performed by the dataplane? (Choose three.)

- A. WildFire updates
- B. NAT
- C. NTP
- D. antivirus
- E. file blocking

Correct Answer: BDE

  **bing2021** 2 months ago

Selected Answer: BDE

mgr plane vs data plane traffic
upvoted 1 times

  **Marshpillowz** 7 months, 2 weeks ago



Selected Answer: BDE

B, D and E are correct
upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: BDE

updates and NTP should be done by management plane in this case
upvoted 2 times


  **ev333** 2 years, 6 months ago

Selected Answer: BDE

Bde correct
upvoted 3 times

  **vj77** 3 years, 4 months ago



can someone please explain this, default port for mgmt services, are we talking about default mgmt interface?
upvoted 2 times

  **dthetinski** 3 years, 4 months ago

Tasks related MGMT services, like, updates, NTP, user-id agent, are performed by control plane. Tasks related to traffic, content-id, app-id, are performed by dataplane.
upvoted 11 times

  **secdaddy** 1 year, 11 months ago

The mention of default port has nothing to do with the question being asked about which services are dataplane.
upvoted 2 times

  **pajonk** 3 years, 4 months ago

Answer B, D, E
upvoted 2 times

An administrator is using Panorama and multiple Palo Alto Networks NGFWs. After upgrading all devices to the latest PAN-OS® software, the administrator enables log forwarding from the firewalls to Panorama. Pre-existing logs from the firewalls are not appearing in Panorama. Which action would enable the firewalls to send their pre-existing logs to Panorama?

- A. Use the import option to pull logs into Panorama.
- B. A CLI command will forward the pre-existing logs to Panorama.
- C. Use the ACC to consolidate pre-existing logs.
- D. The log database will need to be exported from the firewalls and manually imported into Panorama.

Correct Answer: B

Edu147 Highly Voted 5 years, 1 month ago

Correct is B

commands:
request logdb
migrate-to-panorama start end-timestart-timetype
upvoted 30 times

Kane002 Highly Voted 2 years, 9 months ago

I got this question, but the answer was the actual command.

upvoted 6 times

Breyarg 2 years, 8 months ago

how accurate was the rest of these questions for your exam?

upvoted 1 times

bing2021 Most Recent 2 months ago

Selected Answer: B

B, via a command

upvoted 1 times

Marshpillowz 7 months, 2 weeks ago

Selected Answer: B

B is the correct answer

upvoted 1 times

yazid0016 1 year, 8 months ago

B is Correct

upvoted 1 times

lol12 1 year, 10 months ago

Selected Answer: B

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PMD0CAO&refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail>

upvoted 1 times

gully300 1 year, 7 months ago

This is migrating Elastic Search from v2.2 (PAN-OS 9.0) to v5.6 (PAN-OS >9.0), this isn't from a firewall to panorama

upvoted 1 times

JMIB 2 years ago

A CLI command will forward the pre-existing logs to Panorama .. Correct is B

upvoted 1 times

JMIB 2 years ago

Option A is correct.

upvoted 1 times

UFanat 2 years, 2 months ago

Selected Answer: B

Correct is B

commands:
request logdb export


upvoted 2 times

  **dthetinski** 3 years, 4 months ago

B

<https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/set-up-panorama/install-content-and-software-updates-for-panorama/migrate-panorama-logs-to-new-log-format>



upvoted 2 times

  **theroghert** 3 years, 6 months ago

CLI commands: request logdb migrate-to-panorama start end-timestart-timetype

So, B its correct

upvoted 2 times

  **Gabuu** 2 years, 7 months ago

is there a difference between the command you wrote and this : request logdb migrate lc serial-number <ser_num> start

found this command here


<https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/set-up-panorama/install-content-and-software-updates-for-panorama/migrate-panorama-logs-to-new-log-format.html>

upvoted 1 times

  **jonboy22** 2 years, 2 months ago

A new log format is simply which file types the logs are stored as.

upvoted 2 times

  **guilherme_a** 3 years, 11 months ago

correct



upvoted 2 times

A firewall just submitted a file to WildFire for analysis. Assume a 5-minute window for analysis. The firewall is configured to check for verdicts every 5 minutes.

How quickly will the firewall receive back a verdict?

- A. More than 15 minutes
- B. 5 minutes
- C. 10 to 15 minutes
- D. 5 to 10 minutes

Correct Answer: D

  **bing2021** 2 months ago

Selected Answer: D

submit then get back result in 5- 10 mins, study guide
upvoted 1 times

  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: D

Correct answer is D
upvoted 1 times

  **ChiaPet75** 1 year, 3 months ago

Per the PCNSE study notes:

"WildFire Analysis Profiles indicate which files are to be forwarded according to system-wide WildFire configuration settings. WildFire typically renders a verdict on a file within 5 to 10 minutes of receipt."

upvoted 2 times

  **UFanat** 2 years, 2 months ago



Selected Answer: D

It can take 5 to 10 minutes
upvoted 2 times

  **confusion** 2 years, 6 months ago

Selected Answer: D

Submit timestamp + 5min. check for verdicts makes more than 5min. and less than 10min. to get a result.
upvoted 1 times

  **ev333** 2 years, 6 months ago

Selected Answer: D

D is correct
upvoted 1 times























What are the differences between using a service versus using an application for Security Policy match?

- A. Use of a `service` enables the firewall to take immediate action with the first observed packet based on port numbers. Use of an `application` allows the firewall to take immediate action if the port being used is a member of the application standard port list.
- B. There are no differences between `service` or `application`. Use of an `application` simplifies configuration by allowing use of a friendly application name instead of port numbers.
- C. Use of a `service` enables the firewall to take immediate action with the first observed packet based on port numbers. Use of an `application` allows the firewall to take action after enough packets allow for App-ID identification regardless of the ports being used
- D. Use of a `service` enables the firewall to take action after enough packets allow for App-ID identification

Correct Answer: C

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/app-id/app-id-overview>

-   **rocioha** Highly Voted 3 years, 5 months ago
c is correct. <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/app-id/app-id-overview>
upvoted 18 times
-   **bing2021** Most Recent 2 months ago
Selected Answer: C
service cares about port, and app id is based on content
upvoted 1 times
-   **Marshpillowz** 7 months, 2 weeks ago
Selected Answer: C
C is the correct answer
upvoted 1 times
-   **yazid0016** 1 year, 8 months ago
Correct answer is C
upvoted 1 times
-   **lol12** 1 year, 10 months ago
Selected Answer: C
C
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVwCAK>
upvoted 2 times
-   **MyKasala** 2 years, 1 month ago
Selected Answer: C
C is correct
upvoted 2 times
-   **UFanat** 2 years, 2 months ago
C i a correct one
upvoted 2 times
-   **DerekLi23333** 2 years, 3 months ago
Selected Answer: C
Correct answer is C
upvoted 2 times
-   **ramasamymuthiah** 2 years, 4 months ago
Correct answer is C
upvoted 1 times
-   **Rider85** 2 years, 4 months ago
Selected Answer: C
The correct is A. In PcNSE beacon exam is the same question
upvoted 2 times
-   **Rider85** 2 years, 4 months ago
Is C sorry

upvoted 1 times

  **Jared28** 2 years, 5 months ago

PCNSE Beacon practice exam has this exact question, answer C. It's probably a retired question.


upvoted 3 times

  **tururu1496** 2 years, 6 months ago

Selected Answer: C

Answer: C



upvoted 3 times

  **confusion** 2 years, 6 months ago

Selected Answer: C

App ID needs packets to identify the applicaiton.

upvoted 1 times

  **ev333** 2 years, 6 months ago

Selected Answer: C

C is correct this is in all palo marketing materials.

upvoted 1 times

  **unknid** 2 years, 7 months ago

Selected Answer: A



C is incorrect as f, A because this is why you have applipedia, to understand what ports will be allowed on a certan application. If you want port 4433 on ssl, you have to use ssl + service 4433.

upvoted 1 times

  **yogininangpal** 3 years, 4 months ago

Correct answer is C

upvoted 2 times

  **evdw** 3 years, 4 months ago

Correct answer : C

upvoted 2 times

Which Palo Alto Networks VM-Series firewall is valid?

- A. VM-25
- B. VM-800
- C. VM-50
- D. VM-400

Correct Answer: C

Reference:

<https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series>

  **AMARSIL** Highly Voted 4 years, 3 months ago

Correct C
upvoted 7 times

  **Kane002** Highly Voted 2 years, 9 months ago

Probably one of the harder questions. You expect me to remember every single firewall model? Please!
upvoted 6 times

  **GivemeMoney** 2 years, 7 months ago

yeah, what a joke.
upvoted 2 times

  **bing2021** Most Recent 2 months ago

Selected Answer: C

C is correct
upvoted 1 times

  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: C

C is correct
upvoted 1 times

  **[Removed]** 11 months, 1 week ago

Selected Answer: C

VM-50 is correct:
<https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/license-the-vm-series-firewall/vm-series-models>
upvoted 1 times

  **yazid0016** 1 year, 8 months ago

Correct is C
upvoted 1 times

  **KuronekoXIII** 2 years ago

<https://docs.paloaltonetworks.com/vm-series/10-2/vm-series-deployment/license-the-vm-series-firewall/vm-series-models/vm-series-system-requirements#idb04eb16a-3824-4d10-ae65-2f440608f87b>
upvoted 2 times

  **JMIB** 2 years ago

Correct C
upvoted 1 times

  **DerekLi23333** 2 years, 3 months ago

50,100,300,500,700
upvoted 3 times

  **whiteherondance** 2 years, 6 months ago

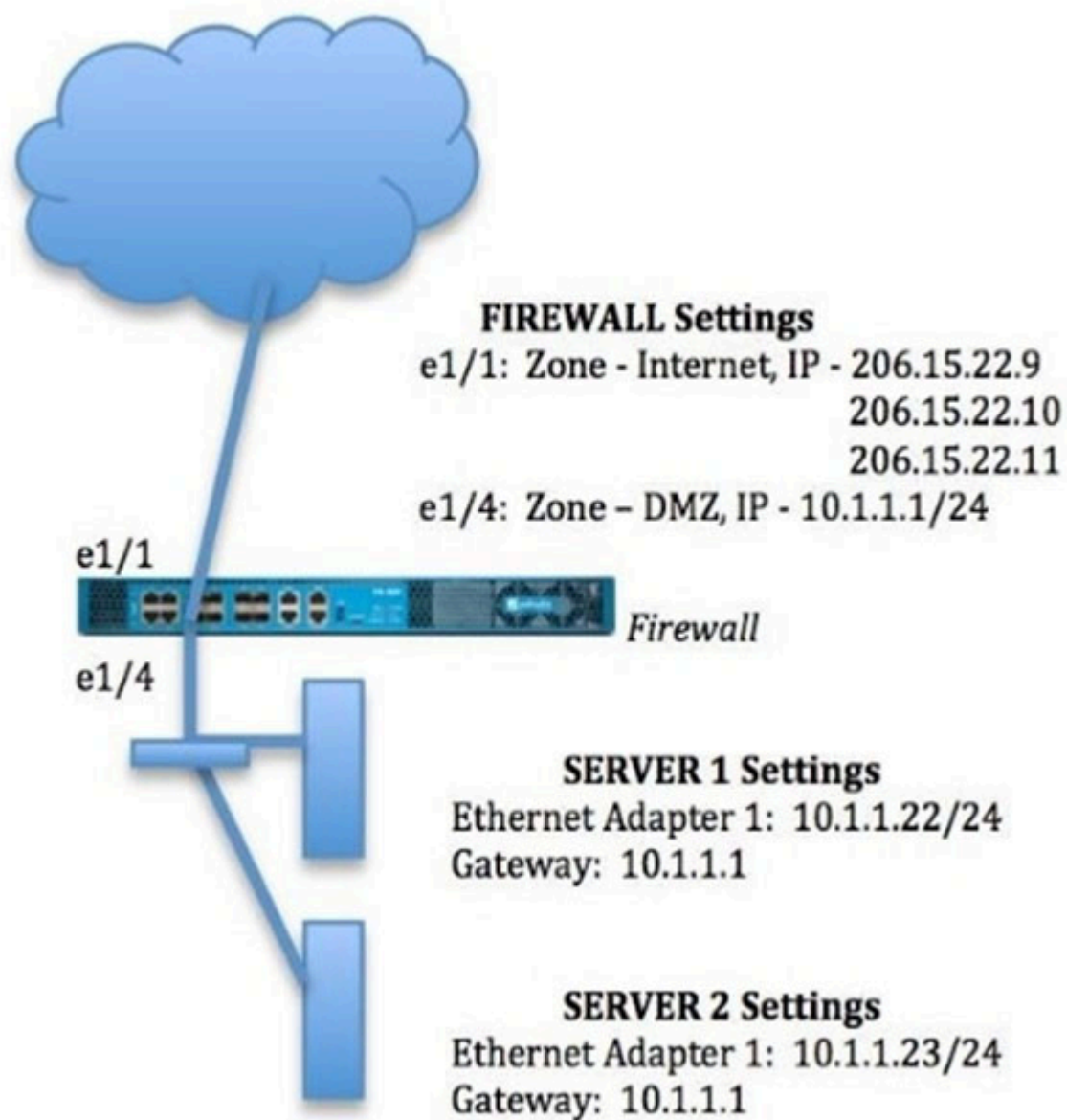
one of the worst questions I've seen in any cert exam...
upvoted 1 times

  **_taintsmasher** 4 years, 4 months ago

Updated reference
<https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/about-the-vm-series-firewall/vm-series-models.html>
upvoted 2 times

An administrator wants multiple web servers in the DMZ to receive connections initiated from the internet. Traffic destined for 206.15.22.9 port 80/TCP needs to be forwarded to the server at 10.1.1.22

Based on the information shown in the image, which NAT rule will forward web-browsing traffic correctly?



A.

Source IP: Any
 Destination IP: 206.15.22.9
 Source Zone: Internet
 Destination Zone: DMZ
 Destination Service: 80/TCP
 Action: Destination NAT
 Translated IP: 10.2.2.23
 Translated Port: 53/UDP

B.

Source IP: Any
 Destination IP: 206.15.22.9
 Source Zone: Internet
 Destination Zone: Internet
 Destination Service: 80/TCP
 Action: Destination NAT
 Translated IP: 10.1.1.22
 Translated Port: 53/UDP

C.

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: None

D.

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 80/TCP

Correct Answer: C

UFanat Highly Voted 2 years, 2 months ago

C is correct. You should distinguish questions for NAT and security rules (the only difference in destination zone - Internet for NAT rules and DMZ for policy rules)
upvoted 12 times

GheeHong 2 years, 2 months ago

Ya, C is correct.
upvoted 1 times

Pakawat 2 years, 1 month ago

Yes, it is C this is NAT rule not security rule.
upvoted 1 times

Kane002 Highly Voted 2 years, 9 months ago

C. NAT zones are just whatever interface traffic is going to. The source (the big cloud internet) is obviously internet, and the destination zone is the internet facing interface of the firewall, so the destination is also internet. It then is translated into an IP that the internal network can read.
upvoted 6 times

bing2021 Most Recent 2 months ago

C is correct, NAT rule interface is before translate, and there is another translate section
upvoted 1 times

Marshpillowz 7 months, 2 weeks ago

C is the correct answer
upvoted 1 times

Pallab_Kundu 1 year, 5 months ago

Correct Answer is D
upvoted 2 times

DatITGuyTho1337 8 months, 3 weeks ago

No, correct answer is C. :)
upvoted 2 times

Jared28 2 years, 6 months ago

C - Based on live production use - Those thinking it is D, if it were not DNAT to a specific port (but all ports), this would be correct (dest zone of the device). However, since a dest svc is specified, it's only translating specific port(s), the destination zone would still be Internet.
upvoted 3 times



HB1989 2 years, 12 months ago

looks like its D, because the destination IP 10.1.1.22 is located in zone DMZ, traffic flow = internet (zone) > DMZ (zone)
upvoted 2 times

HB1989 2 years, 12 months ago


after some test, C is correct.

upvoted 3 times

  **evdw** 3 years, 4 months ago

Correct answer : C

upvoted 1 times

  **frodo1791** 3 years, 4 months ago



Correct answer is C.

upvoted 2 times

  **juli_AZ_900** 3 years, 5 months ago



The answer is D

upvoted 2 times

  **vj77** 3 years, 4 months ago

D is not correct since the NAT zone should be internet to internet; NOT DMZ

upvoted 2 times

  **foromi** 3 years, 5 months ago

The answer is incorrect, because this is a NAT rule and cannot be the DMZ. The correct answer is C.

upvoted 5 times

  **juli_AZ_900** 3 years, 4 months ago

The correct answer is C

upvoted 1 times


An administrator creates a custom application containing Layer 7 signatures. The latest application and threat dynamic update is downloaded to the same NGFW.

The update contains an application that matches the same traffic signatures as the custom application.

Which application should be used to identify traffic traversing the NGFW?

- A. Custom application
- B. System logs show an application error and neither signature is used.
- C. Downloaded application
- D. Custom and downloaded application signature files are merged and both are used

Correct Answer: A

  **hamshoo** Highly Voted 4 years, 2 months ago

Custom applications take precedence over predefined applications when traffic matches both a custom-defined signature and a Palo Alto Networks signature. Accordingly, Traffic logs reflect the custom application name once the new application has been configured.

Answer is A

upvoted 24 times

  **GivemeMoney** 2 years, 7 months ago

straight from here (bottom of page): <https://docs.paloaltonetworks.com/pan-os/u-v/custom-app-id-and-threat-signatures/custom-application-and-threat-signatures/about-custom-application-signatures.html>

Thanks hamshoo

upvoted 4 times

  **Eiffelsturm** 9 months ago

but the question is what SHOULD be used. And the downloaded App should be used for sure

upvoted 2 times

  **kam1967** 7 months ago

I disagree. If the custom application was created for a specific purpose, the new APP-ID that may happen to also match the custom application could be missing critical additions that have been included in the custom app. For this reason, custom apps should always take precedence over new dynamic apps until the new dynamic apps can be examined to ensure they satisfy all of the requirements that the custom apps satisfies.

upvoted 1 times

  **luckymuki** Highly Voted 4 years, 2 months ago

A.

<https://docs.paloaltonetworks.com/pan-os/u-v/custom-app-id-and-threat-signatures/custom-application-and-threat-signatures/about-custom-application-signatures.html>

upvoted 6 times

  **networkingXIV** Most Recent 2 weeks ago

Selected Answer: A

"Custom applications take precedence over predefined applications when traffic matches both a custom-defined signature and a Palo Alto Networks signature. Accordingly, Traffic logs reflect the custom application name once the new application has been configured."

upvoted 1 times

  **BTSeeYa** 1 month, 2 weeks ago

Selected Answer: C

Question states the apps are identical in signatures and asks what "should" be used.

Wouldn't you want Palo Alto modifying and updating that App-ID in the future for you, as it's threat intel teams gather global information, or do you want to do that yourself for various App-IDs?

upvoted 1 times

  **OmarK** 5 months ago

Selected Answer: C

The correct answer is C. Downloaded application. Here's why:

App-ID Prioritization: Palo Alto firewalls prioritize official, vendor-provided application signatures (those downloaded in updates) over custom applications. This ensures that the firewall leverages the most up-to-date and reliable application identification mechanisms.

Conflict Resolution: When a conflict occurs, the firewall will automatically use the downloaded application, overriding the custom application to avoid potential misidentification.

Maintaining Custom Apps: While custom applications are useful for unique traffic not covered by standard applications, it's important to regularly review them against official App-ID updates to avoid conflicts and potential misidentification of traffic.

upvoted 2 times

  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: C

Correct answer is C



upvoted 1 times

  **JoyBoyMx** 1 year ago

Selected Answer: C

I believe the answer is C, as the question says: "What application SHOULD be used", in that case we should use the downloaded app.

upvoted 1 times

  **lol12** 1 year, 10 months ago

Poorly written question. Best practice would be to use the Downloaded application.

I think they're asking for which takes precedence so it will be A.

upvoted 6 times

  **Gngogh** 1 year, 9 months ago

i couldn't agree more

upvoted 3 times

  **UFanat** 2 years, 2 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/u-v/custom-app-id-and-threat-signatures/custom-application-and-threat-signatures/about-custom-application-signatures>

Custom applications take precedence over predefined applications when traffic matches both a custom-defined signature and a Palo Alto Networks signature

upvoted 2 times

  **Jared28** 2 years, 6 months ago

C - As others stated which *SHOULD* be used. If you want the best possible Content-ID inspections, best protection, you *should* use the app defined by PA themselves.

upvoted 4 times

  **kerberos** 2 years, 7 months ago

"Which application SHOULD be used to identify traffic traversing the NGFW?" is the question.

Palo looking for answer C

upvoted 1 times

  **Kane002** 2 years, 9 months ago

C. Custom apps take precedence, but the question is saying that PA has released an App-ID for that app, and therefore the custom application should be deleted and the downloaded app should be used instead.

upvoted 1 times

  **jonboy22** 2 years, 11 months ago

Custom App Sigs DO take precedence over the default downloaded one. But that is not what this question is asking. The questions asks, "SHOULD you use..." and to that effect no, you should not use the custom application any longer. Instead, use the Palo Alto created App Sig.

Answer is C

upvoted 5 times

  **aadach** 3 years, 5 months ago



everything what is custom has the highest priority (precedence)

upvoted 1 times

  **reyesm** 3 years, 7 months ago

A, custom apps take precedence over palo app updates

upvoted 2 times

  **lol1000** 3 years, 10 months ago

If you create a custom app and use it in policy then new apps will not take effect as they are not used.

upvoted 1 times

  **rizky0588** 4 years, 3 months ago

i think correct answer is A

upvoted 2 times

Starting with PAN-OS version 9.1, GlobalProtect logging information is now recorded in which firewall log?

- A. GlobalProtect
- B. System
- C. Authentication
- D. Configuration



Correct Answer: A

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/globalprotect-features/enhanced-logging-for-globalprotect.html>

  **zhawk7661** Highly Voted  4 years, 1 month ago

Correct Answer: A
upvoted 7 times

  **eyelasers1** 2 years, 6 months ago

Source: <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-severity-levels/globalprotect-logs.html>
upvoted 2 times

  **Marshpillowz** Most Recent  7 months, 2 weeks ago

Selected Answer: A

Correct answer is A
upvoted 1 times

  **JMIB** 2 years ago

Correct Answer: A
upvoted 1 times

Refer to the exhibit.

```
#####
```

```
admin@Lab33-111-PA-3060(active)> show routing fib
```

id	destination	nexthop	flags	interface	mtu
47	0.0.0.0/0	10.46.40.1	ug	ethernet1/3	1500
46	10.46.40.0/23	0.0.0.0	u	ethernet1/3	1500
45	10.46.41.111/32	0.0.0.0	uh	ethernet1/3	1500
70	10.46.41.113/32	10.46.40.1	ug	ethernet1/3	1500
51	192.168.111.0/24	0.0.0.0	u	ethernet1/6	1500
50	192.168.111.2/32	0.0.0.0	uh	ethernet1/6	1500

```
#####
```

```
admin@Lab33-111-PA-3060(active)> show virtual-wire all
```

```
total virtual-wire shown : 1
```

```
flags : m - multicast firewalling
        p - link state pass-through
        s - vlan sub-interface
        i - ip+vlan sub-interface
        t - tenant sub-interface
```

name	interface1	interface2	flags	allowed-tags
VW-1	ethernet1/7	ethernet1/5	p	

```
#####
```

Which will be the egress interface if the traffic's ingress interface is ethernet1/7 sourcing from 192.168.111.3 and to the destination 10.46.41.113?

- A. ethernet1/6
- B. ethernet1/3
- C. ethernet1/7
- D. ethernet1/5

Correct Answer: D

Narendragpt Highly Voted 3 years, 5 months ago

D is correct . <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/configure-interfaces/virtual-wire-interfaces.html>
upvoted 10 times

rolmok Highly Voted 2 years, 9 months ago

Correct Ans: D. Virtual Wire would not check the L3 routing information
upvoted 9 times

bing2021 Most Recent 2 months ago

Selected Answer: D

follow vwire output
upvoted 1 times

Marshpillowz 7 months, 2 weeks ago

Selected Answer: D

D is correct here
upvoted 1 times



sov4 1 year, 1 month ago

Selected Answer: D

Question is on the exam. I got this question a few weeks ago... July 2023.
upvoted 1 times

sridot 1 year, 3 months ago

If it's "sourcing from 192.168.111.3" wouldn't that be a source of e6, thus not applying to the vwire?
upvoted 1 times

  **sridot** 1 year, 3 months ago

Apologies, I was misreading things and was worried that there may have been a misprint in the question. D is definitely correct.
upvoted 1 times

  **1Adrian1** 2 years, 5 months ago

B is the correct answer, based on the fib output
upvoted 2 times

  **secdaddy** 1 year, 11 months ago

it's a virtual wire = no fib lookup
upvoted 1 times

  **confusion** 2 years, 6 months ago

Selected Answer: D



It's a vwyre: in 1/7, out 1/5 and vice versa.
upvoted 6 times

  **rocioha** 3 years, 5 months ago



Sorry I was wrong, because of the virtual wire is the 1/5
upvoted 2 times

  **rocioha** 3 years, 5 months ago

B is correct because of the destination and next hoop
upvoted 1 times

  **Raikin** 3 years, 4 months ago

No, because it is virtual wire interface, not layer 3 int.
upvoted 1 times

  **vj77** 3 years, 4 months ago

When an interface is configured as virtual wire, the routing table is not checked by the FW. If it enters one interface, it has to exit the other interface of the virtual wire, there is no exception.
upvoted 7 times

  **shetoshandasa** 3 years, 5 months ago

Correct Answer
upvoted 1 times

Which three authentication services can an administrator use to authenticate admins into the Palo Alto Networks NGFW without defining a corresponding admin account on the local firewall? (Choose three.)

- A. Kerberos
- B. PAP
- C. SAML
- D. TACACS+
- E. RADIUS
- F. LDAP

Correct Answer: CDE

Dabouncer Highly Voted 5 years, 4 months ago

The answer should be C, D, and E

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication>

upvoted 16 times

kerberos Highly Voted 4 years ago

The administrative accounts are defined on an external SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall.

upvoted 10 times

bing2021 Most Recent 2 months ago

Selected Answer: CDE

Idap is not matching questions.

upvoted 1 times

Marshpillowz 7 months, 2 weeks ago

Selected Answer: CDE

C, D and E are correct

upvoted 1 times

JRKhan 7 months, 4 weeks ago

Selected Answer: CDE

CDE are correct. With LDAP, you have to define the admin user locally otherwise there is no other way to assign a role to the user. With Radius, tacacs and saml the firewall can utilise the received VSAs or SAML attributes to map to the roles locally defined on the firewall.

upvoted 1 times

awtsuriticuna 1 year, 9 months ago

The administrative accounts are defined on an external SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication>

upvoted 2 times

1Adrian1 2 years, 5 months ago

A,C,F is the correct answer

upvoted 1 times

confusion 2 years, 6 months ago

Selected Answer: CDE

Without defining user only CDE

upvoted 2 times

Igkhan 2 years, 9 months ago

Selected Answer: CDE

CDE are the correct answers.

upvoted 2 times

👤 **vj77** 3 years, 4 months ago

LDAP is also an answer. I don't understand why NOT, CDEF should be correct. I did LDAP for admin users myself. correct me if I'm wrong.

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/configure-ldap-authentication>

upvoted 1 times

👤 **confusion** 2 years, 6 months ago

Ldap requires user to be defined on the FW for authentication and question asks without configuring user.

upvoted 1 times

👤 **darcone23** 7 months ago

no it doesn't. I have LDAP and RADIUS auth profile and only local admin under administrators :)

upvoted 1 times

👤 **eyelasers1** 2 years, 6 months ago

Per <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication.html> , LDAP can only be used for authentication. The authorization requires that there be a local admin account.

upvoted 2 times

👤 **rocioha** 3 years, 5 months ago

C-D-E <https://origin-docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-administrative-accounts-and-authentication/configure-local-or-external-authentication-for-firewall-administrators.html>

upvoted 1 times

👤 **hpbdc** 3 years, 9 months ago

"...without defining a corresponding admin account on the local firewall?"

so what?! it talks about "authenticate" only! So that means we do not talk about "authorization" here (i.e. role mapping). When it comes to authentication only all of them could be used: ACDEF but.. is that what they wanna see here?

more likely they wanna know which can be used without any need to create a local account at all (i.e even authorization) and that leads to: CDE

according to:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-administrative-accounts-and-authentication/configure-local-or-external-authentication-for-firewall-administrators.html#id7484db35-8218-421b-9847-eab796beea99>

so most likely CDE is what they wanna see here - imho

upvoted 4 times

👤 **PacketFairy** 3 years, 9 months ago

RADIUS does not need an admin configured. VSAs (Vendor specific attributes) would be used.

I log in as Jack, RADIUS sends back a success and a VSA value. If that value corresponds to read/write administrator, I get logged in as a superuser.

There are VSAs for read only and user (Global protect access but not admin). I am unsure what other Auth methods can use VSA or a similar mechanism. If admin users are configured with RADIUS, no need for VSA.

upvoted 1 times

👤 **lol1000** 3 years, 10 months ago

c, d, e

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication.html>

upvoted 1 times

👤 **kambata** 3 years, 10 months ago

Correct answer is C, D and E, please !

upvoted 1 times

👤 **DaveDK** 3 years, 12 months ago

The administrative accounts are defined on an external SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall. For details, see:

upvoted 1 times

👤 **jin3209** 4 years, 2 months ago

what is the right answer for the exam alone?

ACF or CDE?

upvoted 1 times

Which event will happen if an administrator uses an Application Override Policy?

- A. Threat-ID processing time is decreased.
- B. The Palo Alto Networks NGFW stops App-ID processing at Layer 4.
- C. The application name assigned to the traffic by the security rule is written to the Traffic log.
- D. App-ID processing time is increased.

Correct Answer: B

Reference:

<https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-and-Tricks-How-to-Create-an-Application-Override/ta-p/65513>

  **ChiaPet75** Highly Voted 4 years, 2 months ago

Correct: B

"If you define an application override, the firewall stops processing at Layer-4. The custom application name is assigned to the session to help identify it in the logs, and the traffic is not scanned for threats."

(See the bottom of the page)

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/manage-custom-or-unknown-applications>

upvoted 15 times

  **duckduckgoo** 1 year, 4 months ago

updated link

<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/app-id/manage-custom-or-unknown-applications>

upvoted 1 times

  **redgi0** 1 week, 2 days ago

<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/policy/application-override-policy>

upvoted 1 times

  **joe17021991** Highly Voted 4 years, 1 month ago

Alternatively, if you would like the firewall to process the custom application using fast path (Layer-4 inspection instead of using App-ID for Layer-7 inspection), you can reference the custom application in an application override policy rule. An application override with a custom application will prevent the session from being processed by the App-ID engine, which is a Layer-7 inspection. Instead it forces the firewall to handle the session as a regular stateful inspection firewall at Layer-4, and thereby saves application processing time.

upvoted 6 times

  **Prutser2** 3 years, 2 months ago

correct, so this question is all about the wording, with application override, there is no app ID inspection, only statefull. so answer B wording makes it wrong. a side effect of this is that threat inspection is not taking place , so it could be answer A also

upvoted 1 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: B

B is the correct answer

upvoted 1 times

  **tmp99** 1 year ago

B

<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/policy/application-override-policy>

upvoted 1 times

  **Merlin0o** 1 year, 2 months ago

Selected Answer: B

Correct: B

Ref:



<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/application-override-policy>

upvoted 1 times

  **yazid0016** 1 year, 8 months ago

B is correct

upvoted 1 times


  **Gngogh** 1 year, 9 months ago

I do not agree that B is the correct answer, however is the only best choice.
answer A: CTD processing time is not decreased, we can only do it or not
answer B: APP-ID is layer 7 processing not layer 4
answer C: APP name is assigned by the Application override policy not security policy
answer D: There is no APP-ID processing, so the time is not increased
upvoted 3 times

  **SH_** 6 months, 4 weeks ago

I agree. B is correct mainly by elimination. because if the app-ID assigned to the traffic by an Application Override policy rule includes an application signature that has a Parent App based on a non-custom application, then Content-ID (layer 7) inspection of the payload content is possible.

upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: B



Tricky configured question. But it's B. NGFW is not processing at Layer 7 if Application Override Policy is in use for this app. Only Layer 4 processing.

upvoted 1 times

  **NNgiggs** 2 years, 10 months ago


B is the correct Answer, A can not be an option because A talks of reduction in APP ID processing time. there will be no APP ID processing all together so APP ID is out of the question When an override is configured.

upvoted 3 times

  **trashboat** 3 years, 4 months ago

So technically A is also true, but *only for traffic that does not have a pre-defined application.*

upvoted 1 times

  **trashboat** 3 years, 4 months ago

B is the correct answer as application override will stop processing traffic identified as a custom application at/after layer 4, however note the Special Note in the following documentation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVLCA0>



"The exception to this is when you override to a pre-defined application that supports threat inspection."

upvoted 1 times

  **ThomasDao** 3 years, 6 months ago

B - correct

upvoted 1 times

  **joe17021991** 4 years, 1 month ago



Answer is C. App Override stops Layer 7 processing not layer 4.

upvoted 2 times

  **alexblue** 4 years, 1 month ago

because it uses the TCP port as override method, it stops at layer 4


upvoted 3 times

  **lol1000** 3 years, 10 months ago

Correct b.

App-ID stops "at" layer 4.

upvoted 2 times

  **Woody** 1 year, 8 months ago

Agree with Joe. <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/manage-custom-or-unknown-applications>

Vote for C. B is incorrect!

upvoted 1 times

  **rajputparveen** 4 years, 2 months ago

B is correct

upvoted 6 times

Which Security policy rule will allow an admin to block facebook chat but allow Facebook in general?

- A. Deny application facebook-chat before allowing application facebook
- B. Deny application facebook on top
- C. Allow application facebook on top
- D. Allow application facebook before denying application facebook-chat

Correct Answer: A

Reference:

<https://live.paloaltonetworks.com/t5/Configuration-Articles/Failed-to-Block-Facebook-Chat-Consistently/ta-p/115673>

rajputparveen Highly Voted 4 years, 2 months ago

A correct
upvoted 17 times

NNgiggs Highly Voted 2 years, 8 months ago

Allowing Facebook will allow all its dependents including Facebook chat. therefore, you will need to block Facebook chat before the allow Facebook below it. A is the correct answer.
upvoted 6 times

bing2021 Most Recent 2 months ago

Selected Answer: A
before allow fb base
upvoted 1 times

Marshpillowz 7 months, 2 weeks ago

Selected Answer: A
A is the correct answer
upvoted 1 times

Spippolo 1 year, 6 months ago

Selected Answer: A
A is correct
upvoted 2 times

aatechler 1 year, 7 months ago

Selected Answer: A
A >>>Just tested on my LAB.
Deny Face chat
Allow Facebook and DNS
upvoted 5 times

PANW 1 year, 8 months ago

Selected Answer: D
The answer is D:
PANW firewalls do application shifting so it can transition from Facebook-base to facebook-chat and allow everything facebook accept chat
I tried it in my lab with rule order as in answer D: and everything works accept Facebook messenger
I disabled the deny rule and messenger started working again
Proof is in the pudding
upvoted 2 times

sujss 1 year, 7 months ago

But the answer D doesn't really mean allowing everything except chat, it simply says allow FB before denying chat(as far as I understand), meaning 2 separate rules.So if the traffic matches a certain rule the firwall will stop processing the traffic further so would it be able to identify facebook chat when the application shifts. I might be incorrect please help to clarify this. (the answers might not have been properly worded here adding to the confusion).
upvoted 1 times


yazid0016 1 year, 8 months ago

A is correct
upvoted 1 times

JMIB 2 years ago

A is correct

upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: A


A is correct

upvoted 2 times

  **Kane002** 2 years, 9 months ago

C. facebook-chat is dependent on facebook, and must be explicitly allowed. Therefore, permit facebook only, and facebook-chat will fall to the interzone default of deny.



upvoted 2 times

  **Breyarg** 2 years, 8 months ago

if you allow facebook as a parent app then it will allow all sub apps including facebook chat. your answer and logic is incorrect. correct answer is A.



you Deny the facebook chat, then allow all of facebook after.

upvoted 4 times

  **zjam** 3 years, 1 month ago

correct

upvoted 2 times

  **Pag0s** 3 years, 6 months ago

A is correct

upvoted 3 times

A client is concerned about resource exhaustion because of denial-of-service attacks against their DNS servers.

Which option will protect the individual servers?

- A. Enable packet buffer protection on the Zone Protection Profile.
- B. Apply an Anti-Spyware Profile with DNS sinkholing.
- C. Use the DNS App-ID with application-default.
- D. Apply a classified DoS Protection Profile.

Correct Answer: D

  **Edu147** Highly Voted 5 years, 1 month ago

Correct is D

They want to protect just one specific server, if you apply the zone protection you are protecting the entire zone

upvoted 29 times

  **Chris71Mach1** 1 year, 8 months ago

The explanation we all need. Thanks!

upvoted 3 times

  **Ripu** Highly Voted 4 years, 2 months ago

Answer:D

upvoted 5 times

  **Barry_Allen** 3 years, 6 months ago

:D smiling face

upvoted 5 times

  **bing2021** Most Recent 2 months ago

Selected Answer: D

for one specific server

upvoted 1 times

  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: D

D is correct


upvoted 1 times

  **[Removed]** 1 year, 2 months ago

Correct is D

DOS protection if for resources behind the firewall. Zone Protection is for the firewall.

upvoted 2 times

  **Pochex** 1 year, 6 months ago

Answer D is the correct one. Classified profiles protect individual critical resources, especially servers that users access from the internet, and are often attack targets, such as web servers, database servers, and DNS servers.

Please refer to <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules/classified-versus-aggregate-dos-protection>

upvoted 1 times

  **yazid0016** 1 year, 8 months ago



Correct answer : D

upvoted 1 times

  **yazid0016** 1 year, 8 months ago

Correct answer is D

upvoted 1 times

  **Woody** 1 year, 8 months ago

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules/classified-versus-aggregate-dos-protection#id56c14277-0ecd-4e32-b3d3-7b616176204a>



D.

upvoted 3 times

  **UFanat** 2 years, 2 months ago

Selected Answer: D

D. Apply a classified DoS Protection Profile.
upvoted 1 times

  **Igkhan** 2 years, 9 months ago



Selected Answer: D

D is correct.
upvoted 2 times

  **Kane002** 2 years, 9 months ago

Selected Answer: D



D. Single protection is for DoS.
upvoted 3 times

  **zuby76** 2 years, 10 months ago

D is the right answer
Packet Buffer protection is indeed the way to protect against resource exhaustion, but it is not configured under DoS protection profile. It is directly enabled under Zones.
upvoted 3 times

  **chris_fgt** 3 years ago

D is the correct answer
upvoted 1 times

  **Zabol** 3 years, 2 months ago

Definitely D is correct
upvoted 1 times

  **YasserSaied** 3 years, 2 months ago

D -- it couldn't be else
upvoted 1 times

  **yogininangpal** 3 years, 4 months ago

D is the correct answer, for specific servers not the entire zone so correct answer is not A
upvoted 1 times

If the firewall is configured for credential phishing prevention using the `Domain Credential Filter` method, which login will be detected as credential theft?

- A. Mapping to the IP address of the logged-in user.
- B. First four letters of the username matching any valid corporate username.
- C. Using the same user's corporate username and password.
- D. Matching any valid corporate username.

Correct Answer: C

  **Silent_Sanctuary** Highly Voted 4 years, 3 months ago

Correct Answer is C

The Windows-based User-ID agent is installed on a Read-Only Domain Controller (RODC). The User-ID agent collects password hashes that correspond to users for which you want to enable credential detection and sends these mappings to the firewall. The firewall then checks if the source IP address of a session matches a username and if the password submitted to the webpage belongs to that username. With this mode, the firewall blocks or alerts on the submission only when the password submitted matches a user password.

upvoted 13 times

  **Sammy3637** Highly Voted 4 years, 8 months ago

correct answer is C



upvoted 5 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: C

Correct answer is C



upvoted 1 times

  **JRKhan** 7 months, 4 weeks ago

Selected Answer: C

C is correct. With Domain credential method, firewall check both the username and password submitted on the untrusted/potentially phishing website.

upvoted 1 times

  **lol12** 1 year, 10 months ago

Selected Answer: A

I think it's A.

Domain Credential Filter - To verify that the credentials belong to the login username—The firewall looks for a mapping between the IP address of the login username and the detected username in its IP address-to-username mapping table.

upvoted 1 times

  **JMIB** 2 years ago

C is a correct.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/url-filtering/prevent-credential-phishing/methods-to-check-for-corporate-credential-submissions>

upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: C

C is a correct. A - for ip user mapping not domain

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/url-filtering/prevent-credential-phishing/methods-to-check-for-corporate-credential-submissions>

upvoted 2 times

  **tenebrox** 2 years, 2 months ago

Selected Answer: C

Correct Answer is C

upvoted 2 times

  **Jared28** 2 years, 5 months ago

Selected Answer: C

In PCNSE Beacon Practice exam, confirms C but likely retired

upvoted 3 times

  **wmelo** 3 years, 1 month ago

Correct Answer C

Use Domain Credential Filter—Checks for valid corporate usernames and password submissions and verifies that the submitted credentials match the user logged into the source IP address of the session.

Link: <https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-new-features/content-inspection-features/credential-phishing-prevention>
upvoted 2 times

  **nashwan19** 3 years, 2 months ago

C is the correct answer

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-credential-phishing/methods-to-check-for-corporate-credential-submissions.html#id29eff481-13de-45b9-b73c-83e2e932ba20>

upvoted 2 times

  **YasserSaied** 3 years, 2 months ago


C -- is the correct answer

upvoted 1 times

  **yogininangpal** 3 years, 4 months ago

What is the question that is being asked does the question ask about if Domain credential filter is implemented how does the credential theft detected then the answer is C, maybe Palo needs to get people to write exam questions correctly and ask what they really mean!! There is no reason to ask trick question when you are trying to test knowledge for the product!!


upvoted 1 times

  **trashboat** 3 years, 4 months ago

C is the answer, since the question asks about Domain Credential Filter credential checking.

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/url-filtering/prevent-credential-phishing/methods-to-check-for-corporate-credential-submissions.html#id29eff481-13de-45b9-b73c-83e2e932ba20>

upvoted 1 times

  **jordan_gsi** 3 years, 5 months ago

read carefully, question it self said using "Domain Credential Filter method" if you are using that method :

detects whether a user is submitting a valid username and password and that those credentials match the user who is logged in to the source IP address of the session, Configure Credential Detection with the Windows-basedUser-IDAgent and Map IP Addresses to Users.

but if you are using IP user mapping method A: would be the right answer,

below the KB

Enjoy!



<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-new-features/content-inspection-features/credential-phishing-prevention>

upvoted 2 times

  **reyesm** 3 years, 7 months ago

Use Domain Credential Filter—Checks for valid corporate usernames and password submissions and verifies that the username maps to the IP address of the logged in user.

upvoted 1 times

  **trykali** 3 years, 8 months ago

The answer is C,

IP-User: This credential detection method checks for valid username submissions. You can use this method to detect credential submissions that include a valid corporate username (regardless of the accompanying password).

Domain Credential: This credential detection method enables the firewall to check for a valid corporate username and the associated password. The firewall determines if the username and password a user submits matches the same user's corporate username and password.

upvoted 2 times

An administrator has users accessing network resources through Citrix XenApp 7.x.

Which User-ID mapping solution will map multiple users who are using Citrix to connect to the network and access resources?

- A. Client Probing
- B. Terminal Services agent
- C. GlobalProtect
- D. Syslog Monitoring

Correct Answer: B

  **Mello** Highly Voted 4 years, 10 months ago

The correct answer may be B

<https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/user-id/map-ip-addresses-to-users>

upvoted 8 times

  **bing2021** Most Recent 2 months ago

Selected Answer: B

citrix, terminal agent



upvoted 1 times

  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

  **omgt2k2** 7 months, 4 weeks ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/user-id/user-id-concepts/user-mapping/port-mapping>

upvoted 1 times

  **[Removed]** 1 year, 5 months ago

B

In environments with multi-user systems—such as Microsoft Terminal Server or Citrix environments—many users share the same IP address. In this case, the user-to-IP address mapping process requires knowledge of the source port of each client. To perform this type of mapping, you must install the Palo Alto Networks Terminal Server Agent on the Windows/Citrix terminal server itself to intermediate the assignment of source ports to the various user processes. For terminal servers that do not support the Terminal Server agent, such as Linux terminal servers, you can use the XML API to send user mapping information from login and logout events to UserID. See Configure User Mapping for Terminal Server Users for configuration details.

upvoted 3 times

  **duckduckgoo** 1 year, 4 months ago

And here is the link.

<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/user-id/user-id-concepts/user-mapping/port-mapping>

upvoted 1 times

  **JMIB** 2 years ago

B is correct

upvoted 1 times

  **juangsap** 2 years, 2 months ago

B



<https://docs.paloaltonetworks.com/compatibility-matrix/terminal-services-ts-agent/terminal-services-ts-agent-table#id17CBA50079Z>

upvoted 1 times

  **Narendragpt** 3 years, 5 months ago



B is correct - If you have clients running multi-user systems in a Windows environment, such as Microsoft Terminal Server or Citrix Metaframe Presentation Server or XenApp, Configure the Palo Alto Networks Terminal Server (TS) Agent for User Mapping.

upvoted 4 times

  **DJNhunzi** 3 years, 10 months ago

B is correct

upvoted 2 times

  **lol1000** 3 years, 10 months ago

b

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/user-id/map-ip-addresses-to-users.html>

upvoted 1 times

  **tech_catarina_mall** 4 years ago

Correct answer is B: Terminal Service Agent



<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-ip-addresses-to-users.html>

upvoted 1 times

  **PacketFairy** 3 years, 9 months ago



Citrix is a terminal server. Each user is allocated a pool of source ports. Everybody logged in has the same IP so the only way to differentiate is by tcp/udp source port. This is what the terminal service agent does.

upvoted 4 times

  **KAACK** 4 years, 1 month ago

answer is B

upvoted 2 times

  **Ripu** 4 years, 2 months ago

Answer:B

upvoted 1 times

  **asmaam** 4 years, 5 months ago

Correct ans = B

upvoted 2 times

  **khalmrj** 4 years, 6 months ago

Correct is B

upvoted 2 times

  **Edu147** 5 years, 1 month ago

Correct is B

upvoted 4 times

  **tester12** 4 years, 11 months ago

Do you have the reference ?

upvoted 2 times

An administrator needs to upgrade a Palo Alto Networks NGFW to the most current version of PAN-OS® software. The firewall has internet connectivity through an Ethernet interface, but no internet connectivity from the management interface. The Security policy has the default security rules and a rule that allows all web- browsing traffic from any to any zone.

What must the administrator configure so that the PAN-OS® software can be upgraded?

- A. Security policy rule
- B. CRL
- C. Service route
- D. Scheduler

Correct Answer: C

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clp3CAC>

  **Edu147** Highly Voted 5 years, 1 month ago

Correct C

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clp3CAC>

upvoted 18 times

  **bing2021** Most Recent 2 months ago

Selected Answer: C

service route, pick dp interface.

upvoted 1 times

  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: C

C is correct



upvoted 1 times

  **TeachTrooper** 7 months, 2 weeks ago

Selected Answer: C

Mentioning the extra security rule is just to trick us into picking A. The default ruleset has an intrazone rule that allows any/any. So if the service route points to the ethernet interface providing the internet connection all paloalto-updates etc. requests will be allowed by the default intrazone policy.



upvoted 1 times

  **Caglart** 9 months, 3 weeks ago

Selected Answer: C

Correct C

upvoted 1 times

  **sov4** 1 year, 1 month ago

Selected Answer: C

C. intra-zone default rule takes care of the security rule since it'll be sourced from the ethernet interface. Only thing left is the service route.

upvoted 1 times

  **Pretorian** 2 years, 1 month ago

This one is another typical PANW malicious test question. We all know that a service route is needed. However, the question states web-browsing is being allowed by the policy. PANW updates are not delivered over web-browsing. Therefore, a new security policy must be added allowing app-ID "paloalto-updates", ssl, and web-browsing on application default service/port.

Just something to consider.


In summary, I'm not sure if "C" is the correct answer, or "A"

upvoted 4 times

  **secdaddy** 1 year, 11 months ago

Also we know that without the service route it clearly will not work so C is the best answer.

upvoted 2 times

  **secdaddy** 1 year, 11 months ago

"...and a rule that allows all web- browsing traffic from any to any zone."



There's no mention of app-ID in the question and from this we know that http(s) are allowed outgoing.

upvoted 1 times

  **rocioha** 3 years, 5 months ago



C Correct

upvoted 4 times

  **shane** 3 years, 6 months ago


Answer:C

upvoted 3 times

  **Yelam** 3 years, 7 months ago



C is correct answer

upvoted 2 times

  **PacketFairy** 3 years, 9 months ago

The management port is an isolated host interface. By default, everything uses this port (DNS, Auth, NTP, updates). If this port has no internet access, "service routes" can be used to perform these services on a router/firewall interface.



upvoted 1 times

  **lol1000** 3 years, 10 months ago

C

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clp3CAC>



upvoted 1 times

  **KAAC** 4 years, 1 month ago

C: Service Route



<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clp3CAC>

upvoted 3 times

  **Giox** 4 years, 2 months ago



The correct answer is A. Surely the Service Route should be configured to use the Ethernet interface, but from the question we cannot say if it is already configured. Instead, we know about configured security policy rule, and using a data interface we need a policy to permit "paloalto-updates" application, that is missing

upvoted 4 times

  **Giox** 4 years, 2 months ago

Sorry, traffic should be allowed by the intrazone default policy rule, so C is the correct one.

upvoted 3 times

  **Ripu** 4 years, 2 months ago

Answer:C

upvoted 1 times

  **datasec919** 4 years, 2 months ago

we can add security rule for management interface IP. so i think correct option is A

upvoted 2 times

  **Silent_Sanctuary** 4 years, 3 months ago

Correct Answer is C

Service Route > Palo Alto Networks Services > Internet/Untrust Zone

upvoted 1 times

Which feature prevents the submission of corporate login information into website forms?

- A. Data filtering
- B. User-ID
- C. File blocking
- D. Credential phishing prevention

Correct Answer: D

Reference:

<https://www.paloaltonetworks.com/cyberpedia/how-the-next-generation-security-platform-contributes-to-gdpr-compliance>

  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: D

D is correct

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-credential-phishing#:~:text=Credential%20phishing%20prevention%20works%20by,submissions%20against%20valid%20corporate%20credentials>
upvoted 1 times

  **DatITGuyTho1337** 8 months, 3 weeks ago

Reckon the answer is indeed "D". If the question asked how credential phishing prevention works then we can bring up User-ID. User-ID is the engine of how credential phishing prevention works. At least that's how I see it.

upvoted 1 times

  **Pallab_Kundu** 1 year, 5 months ago

Selected Answer: D

The feature that prevents the submission of corporate login information into website forms is D. Credential phishing prevention.

Credential phishing prevention is a feature that is designed to protect against phishing attacks, where attackers attempt to trick users into giving away their login credentials. One way this is achieved is by preventing the submission of corporate login information into website forms. When a user enters their credentials into a website form, the firewall can use various methods to detect whether the login is legitimate or a phishing attempt.

upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: D

Only D :)

upvoted 2 times

  **Bubu3k** 2 years, 5 months ago

Selected Answer: D

"Credential phishing prevention works by scanning username and password submissions to websites and comparing those submissions against valid corporate credentials."

From the study guide, page 98

upvoted 3 times

  **Kane002** 2 years, 9 months ago

Looking too deep into an easy question. Credential Phishing Prevention is the name of the feature, D.

upvoted 2 times

  **Biz90** 2 years, 10 months ago

Hi Team,

I would agree this B only reading how this sentence from 10.0: 'you must configure both User-ID to detect when users submit valid corporate credentials to a site'.

Looking at the question it does state about 'Company' credentials.

upvoted 3 times

  **CyberRasta** 2 years, 11 months ago

It is B because "Prevent Credential Phishing" is just the name of the doc, the actual features used are User ID and URL Filtering Profiles.

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/prevent-credential-phishing.html>

upvoted 2 times

  **ochc** 3 years, 9 months ago



Q69 is almost the same, and the answer on that one is "URL Filtering profile". As per <https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/url-filtering/prevent-credential-phishing/set-up-credential-phishing-prevention.html>, steps are 1. User-ID, 2. URL Filtering Profile... 4. Within URL Filtering select "User Credential Detection", not "Credential phishing prevent". So this ans should be B User ID.

upvoted 3 times

  **PlebLord** 3 years, 9 months ago

The key part of this question is "feature", so it should be B as User-ID is a feature whereas Credential Phishing Prevention is just a title of an article related to the concept.

upvoted 3 times

  **duyvo** 3 years, 7 months ago

D is correct. Credential Phishing Prevention is a new feature on PAN-OS 8.0

upvoted 1 times

  **AMARSIL** 4 years, 3 months ago

true is D

upvoted 3 times

Which option is part of the content inspection process?

- A. Packet forwarding process
- B. SSL Proxy re-encrypt
- C. IPsec tunnel encryption
- D. Packet egress process

Correct Answer: B

— **Edu147** Highly Voted 5 years, 1 month ago
Correct B

<http://live.paloaltonetworks.com//t5/image/serverpage/image-id/12862i950F549C7D4E6309>
upvoted 20 times

— **KAACK** Highly Voted 4 years, 1 month ago

B: SSL Proxy re-encrypt
is a process where SSL traffic is decrypted inspected and then re-encrypted to be delivered to the destination.
upvoted 10 times

— **bing2021** Most Recent 2 months ago

Selected Answer: B
proxy re-encryption
upvoted 1 times

— **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: B
Correct answer is B
upvoted 1 times

— **Gabuu** 2 years, 1 month ago

I believe B is the correct answer
upvoted 1 times

— **bmarks** 3 years, 6 months ago

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVHCA0>
Packet Flow Sequence
A occurs during Forwarding/Egress
B occurs during Content Inspection
C occurs during Forwarding/Egress
D occurs during Forwarding/Egress
* The only option part of the Content Inspection Process is [B] SSL Proxy Re-encrypt
ANSWER = [B]
upvoted 10 times

— **Sarbi** 3 years, 9 months ago

Correct A
upvoted 1 times

— **htuna** 4 years ago

Ans. = B
upvoted 2 times

— **asmaam** 4 years, 5 months ago

Correct ans = B
upvoted 4 times

— **EA** 4 years, 11 months ago

Correct B
upvoted 4 times

In a virtual router, which object contains all potential routes?

- A. MIB
- B. RIB
- C. SIP
- D. FIB

Correct Answer: B

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/networking/virtual-routers>

  **john_bosco_champion** Highly Voted 4 years, 2 months ago

For a router, there is the Routing Information Base (RIB) and the Forwarding Information Base (FIB). The difference between these two is that while the RIB contains all possible routes to various destinations, even if, there are more than one to a specific destination, the FIB contains only the best route to each destination. So in this case, the answer is B which is RIB.

upvoted 23 times

  **Sammy3637** Highly Voted 4 years, 8 months ago

Correct is B , it says ALL potential routes , FIB doesn't have all

upvoted 18 times

  **Rim007** 4 years, 6 months ago

RIB is correct, I agree.

upvoted 4 times

  **bing2021** Most Recent 2 months ago

Selected Answer: B

rib is the table has all candidate route

upvoted 1 times

  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/virtual-routers/virtual-router-overview>

upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: B

Correct is B

RIB contains all potential routes

FIB contains all actual (active at the moment) routes

upvoted 1 times

  **jonboy22** 2 years, 2 months ago



BRING OUT THE RIB!

upvoted 1 times

  **fxgoat98** 3 years, 2 months ago

RIB IS CORRECT

upvoted 2 times

  **lol1000** 3 years, 10 months ago

B is correct. RIB has all FIB has active

upvoted 2 times

  **adegboyegaore** 4 years, 3 months ago

B is correct

upvoted 2 times

  **prseedd** 4 years, 4 months ago

B is correct
upvoted 4 times

  **khalmrj** 4 years, 6 months ago

Correct is B
upvoted 4 times

  **dilibabu** 4 years, 8 months ago

Option D FIB
upvoted 1 times

An administrator creates an SSL decryption rule decrypting traffic on all ports. The administrator also creates a Security policy rule allowing only the applications

DNS, SSL, and web-browsing.

The administrator generates three encrypted BitTorrent connections and checks the Traffic logs. There are three entries. The first entry shows traffic dropped as application Unknown. The next two entries show traffic allowed as application SSL.

Which action will stop the second and subsequent encrypted BitTorrent connections from being allowed as SSL?

- A. Create a decryption rule matching the encrypted BitTorrent traffic with action λ No-Decrypt, λ and place the rule at the top of the Decryption policy.
- B. Create a Security policy rule that matches application λ encrypted BitTorrent λ and place the rule at the top of the Security policy.
- C. Disable the exclude cache option for the firewall.
- D. Create a Decryption Profile to block traffic using unsupported cyphers, and attach the profile to the decryption rule.

Correct Answer: D

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRtCAK>

  **ChiaPet75** Highly Voted 4 years, 2 months ago

D is Correct

There is no application called "encrypted BitTorrent" so "B" is not the correct answer. If the application was just "BitTorrent" then "B" would be correct.

"A" would not work either since you would still need to create a Decryption Profile which is not mentioned.

"D" is the most complete answer which is to create the Decryption Profile and attach it to the Decryption rule.

I found a PaloAlto KB article about blocking Tor traffic using a Decryption Profile that is blocking Unsupported cipher's, expired certificates, etc.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRtCAK>

upvoted 20 times

  **lol1000** Highly Voted 3 years, 10 months ago

D is the least wrong

upvoted 9 times

  **davedrangus** 1 week, 6 days ago

I love this response lol. Most of the answers can be defined this way.

upvoted 1 times

  **hcir** Most Recent 2 months, 3 weeks ago

for some reason, the first bittorrent connection was not recognised by app-id as neither dns, ssl nor http. Hence, it was dropped. The other 2 were ssl, and they were not decrypted, so they went through. Because decryption was supposed to decrypt everything, the only reason it was not decrypted can only be related to decryption cypher suite incompatibility. Hence, the answer is D.



upvoted 2 times

  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: D

D appears to be correct

upvoted 1 times

  **JRKhan** 7 months, 4 weeks ago

Selected Answer: D

Most suitable answer is D. The firewall couldnt decrypt the traffic probably because of the use of unsupported ciphers hence the reason in subsequent packets the application is identified as SSL. If the firewall was able to decrypt the traffic, even if it couldnt identify the application it would mark the traffic as web-browsing and not SSL.

upvoted 1 times

  **ThelioNN** 1 year, 3 months ago

Guys, why not A. Seems correct, the FW will leave the bittorrent as bittorrent and block it. Instead of decrypting it. Are we sure the Bittorrent crypto is going to use unsupported ciphers (as that can easily be fixed from the developers)?

upvoted 1 times

  **FaheemParakkot** 1 year ago



As per the question, the first packet is identified as UnKnown Application. Which means, even if you created a rule for BitTorrent, it wont match.

upvoted 1 times

  **Kjohnsting** 1 year, 7 months ago

Don't love this kind of question. Seems incomplete.

upvoted 4 times

  **UFanat** 2 years, 2 months ago

Selected Answer: D

D - correct. You need to fix decryption options, not security policy rule.



upvoted 2 times

  **AbuHussain** 2 years, 5 months ago

Selected Answer: D

answer is D

upvoted 2 times

  **Gabuu** 2 years, 7 months ago



D is correct

upvoted 2 times

  **Kane002** 2 years, 9 months ago

The administrator has created a decryption policy, but bittorrent is slipping past it, only being detected as "ssl", so the admin needs to create a decryption profile to block the evasive behavior, probably bittorrent is using an unsupported cipher, hence the decryption policy failure. D.

upvoted 4 times

  **Zabol** 3 years, 2 months ago

I think it is D, App-ID doesn't have Encrypted-Bittorrent

upvoted 1 times

  **trashboat** 3 years, 4 months ago

D is correct:

B is not correct because the reason the two other sessions are showing allowed as SSL is because they are not being decrypted, otherwise they would be recognized as tor/unknown application and not allowed on the security policy rule. The likely reason for this is they are using unsupported ciphers/etc. - so the answer is D.

C is not relevant.

A is also not correct because the goal is to decrypt the traffic to identify it, so this is the opposite of what is trying to be accomplished.

upvoted 2 times

  **frodo1791** 3 years, 4 months ago


B is not correct... as "encrypted bittorrent" doesn't exist in app-id. So I should go D...

upvoted 2 times

  **hpbdc** 3 years, 9 months ago

check <https://appliedia.paloaltonetworks.com/> there is no app encrypted bittorrent. other then that the rest is clear so D.

upvoted 1 times

  **Pb1805** 4 years, 3 months ago

Correct answer is D

upvoted 1 times

  **Silent_Sanctuary** 4 years, 3 months ago

D is correct

Block sessions that use cipher suites you don't support. You configure which cipher suites (encryption algorithms) to allow on the SSL Protocol Settings tab. Don't allow users to connect to sites with weak cipher suites.

upvoted 2 times

Refer to the exhibit.

Device Certificates		Default Trusted Certificate Authorities							
Name	Subject	Issuer	CA	Key	Expires	Status	Algorithm	Usage	
Domain-Root-Cert	CN = demo.local	CN = demo.local	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Nov 1 00:34:47 2021 GMT	valid	RSA	Trusted Root CA Certificate	
Domain Sub-CA	CN = sub.demo.local	CN = demo.local	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 6 20:59:38 2019 GMT	valid	RSA		
Forward_Trust	CN = fwdtrust.demo.local	CN = sub.demo.local	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 6 21:09:49 2018 GMT	valid	RSA		

Which certificates can be used as a Forward Trust certificate?

- A. Certificate from Default Trust Certificate Authorities
- B. Domain Sub-CA
- C. Forward-Trust
- D. Domain-Root-Cert

Correct Answer: B

Breyarg Highly Voted 2 years, 8 months ago

wouldn't the only correct answer be B?

Must be a CA to be used. must have private key also. can be a root but doesnt have to be.... so that only leaves B as correct answer? anyone? as far as i know you cant use public certs for decryption? so cant be A

upvoted 9 times

NHANTON 2 years, 7 months ago

yes, CA and the key is mandatory

upvoted 4 times

GivemeMoney 2 years, 7 months ago

Should be D. Domain-Root-Cert, the usage "Trusted Root CA Certificate" is the one that is going to be used.

upvoted 2 times

Knowledge33 1 year, 3 months ago

There is no key on the D. The question is "can be used", not "is used". We only need to click on the certificate, then check the box "Forward trust Certificate". Only B is correct.

upvoted 1 times

Pretorian 2 years, 1 month ago

You are correct. You cannot use certificates from well known third party CA's (like GoDaddy, etc) for decryption. The more elegant approach for SSL Forward Proxy and the easiest by far is a to use a domain CA because automatically all domain joined machines will trust those certificates, overcoming the challenge of distribution of the decryption certificate.

upvoted 3 times

Marshpillowz Most Recent 7 months, 2 weeks ago

Selected Answer: B

Correct answer is B

upvoted 1 times

JRKhan 7 months, 4 weeks ago

Selected Answer: B

B is correct as both CA and Key options need to be selected/enabled.

upvoted 1 times

Gabbranch 9 months, 2 weeks ago

Selected Answer: B

Aside from requiring it to be a CA, you'll notice that answer C uses a hyphen but the cert name has an underscore.

upvoted 2 times

  **PaloSteve** 1 year, 1 month ago

My vote is for C.

<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/decryption/configure-ssl-forward-proxy>

In Step 4 of the Use a self-signed certificate as the Forward Trust certificate, which is titled "Generate new subordinate CA certificates for each firewall" it follows with 5. "Click the new certificate to modify it and click the Forward Trust Certificate checkbox to configure the certificate as the Forward Trust Certificate".

The CA box is only necessary to be checked for the Intermediate key. It is the cert created from the Intermediate CA that is used as the Forward Trust cert.



upvoted 2 times

  **Knowledge33** 1 year, 3 months ago

Selected Answer: B



There is no key on the D. The question is "can be used", not "is used". We only need to click on the certificate, then check the box " Forward trust Certificate". Only B is correct.

upvoted 1 times

  **KKQQ12345** 2 years ago

This is not a valid question. Forward-Trusted Cert has to be configured, otherwise you can't even commit.

upvoted 2 times

  **KKQQ12345** 2 years ago

Selected Answer: D

B should be wrong because their usage is empty

AC does not have CA

upvoted 1 times

  **Knowledge33** 1 year, 3 months ago

There is no key on the D. The question is "can be used", not "is used". We only need to click on the certificate, then check the box " Forward trust Certificate". Only B is correct.

upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: B

B is a correct one

upvoted 1 times

  **Meira088** 2 years, 3 months ago

Selected Answer: B

B is correct answer

upvoted 2 times

  **1Adrian1** 2 years, 5 months ago

B is correct



upvoted 2 times

  **NHANTON** 2 years, 7 months ago

Selected Answer: B

B is correct answer

upvoted 4 times

  **poiuytr** 2 years, 4 months ago

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PMNKCA4&lang=en_US%E2%80%A9

upvoted 4 times

  **NHANTON** 2 years, 7 months ago

B is correct answer

upvoted 3 times

Which option would an administrator choose to define the certificate and protocol that Panorama and its managed devices use for SSL/TLS services?

- A. Configure a Decryption Profile and select SSL/TLS services.
- B. Set up SSL/TLS under Policies > Service/URL Category > Service.
- C. Set up Security policy rule to allow SSL communication.
- D. Configure an SSL/TLS Profile.

Correct Answer: D

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-certificate-management-ssl-tls-service-profile>

  **rajputparveen** Highly Voted  4 years, 2 months ago

D is correct one
upvoted 6 times

  **lol1000** Highly Voted  3 years, 10 months ago

d
<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-web-interface-help/device/device-certificate-management-ssl-tls-service-profile.html>
upvoted 5 times

  **Marshpillowz** Most Recent  7 months, 2 weeks ago

Selected Answer: D

D is correct
upvoted 1 times

Which menu item enables a firewall administrator to see details about traffic that is currently active through the NGFW?

- A. ACC
- B. System Logs
- C. App Scope
- D. Session Browser

Correct Answer: D

Marshpillowz 7 months, 2 weeks ago

Selected Answer: D

D is correct
upvoted 1 times

Pallab_Kundu 1 year, 5 months ago

Selected Answer: D

The menu item that enables a firewall administrator to see details about traffic that is currently active through the NGFW is option D: Session Browser.

The Session Browser is a tool in the Palo Alto Networks NGFW web interface that allows administrators to view and monitor active sessions on the firewall. The Session Browser displays a list of active sessions, including the source and destination IP addresses, the application, the security rule that allowed the traffic, and other details.

Using the Session Browser, administrators can search for specific sessions using various criteria, such as source or destination IP address, application, or security rule. They can also filter and sort the sessions based on different attributes, and view detailed information about each session, such as the number of bytes sent and received, the session ID, and the start and end times.

The Session Browser is a useful tool for troubleshooting network issues and monitoring network activity in real-time.

upvoted 2 times

Goharam 1 year, 9 months ago

Session Browser is the answer.

upvoted 1 times

trashboat 3 years, 4 months ago

D is correct - Session browser. However ACC will show metadata on traffic through the firewall, and you can create some helpful on-the-fly reports, but these will not provide deep detail. Alternatively for more detail you can go to Monitor > Traffic and filter for relevant sessions.

upvoted 3 times

frodo1791 3 years, 4 months ago

D is correct.. as it shows the active sessions.

upvoted 4 times

rammsdoct 4 years, 3 months ago

not very clear, but I guess that closer it is D, show session all (CLI)

upvoted 3 times

Breyarg 3 years, 8 months ago

it is very clear. from GUI you can go straight to the session browser under monitoring tab to see current sessions. Answer is 100% D

all other options there will only show ended sessions or started sessions but not the whole active session.

upvoted 5 times

AMARSIL 4 years, 3 months ago

correct answer : D

upvoted 4 times

Which protection feature is available only in a Zone Protection Profile?

- A. SYN Flood Protection using SYN Flood Cookies
- B. ICMP Flood Protection
- C. Port Scan Protection
- D. UDP Flood Protections

Correct Answer: C

  **tester12** Highly Voted 4 years, 11 months ago

Answer seems like is C
upvoted 11 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: C

Correct answer is C
upvoted 1 times

  **Pretorian** 2 years, 1 month ago

I agree with C, however, why not "A"?

Flood protection - SYN cookies is a protection that is only in the Zone Protection

upvoted 2 times

  **secdaddy** 1 year, 11 months ago

Also available via DoS classified so not only Zone Protection

upvoted 1 times

  **duckduckgoo** 1 year, 5 months ago

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CljjCAC>



upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: C



C. Port Scan Protection

upvoted 1 times

  **Breyarg** 2 years, 8 months ago



Done this a million times... def C!

upvoted 3 times

  **Qintao** 3 years, 4 months ago

definitely C

upvoted 2 times



  **mzzzzz** 3 years, 5 months ago

Correct C:

SYN Flood Cookies is also available on DoS Protection Profile, the answer refers to ONLY.



DoS Protection profiles protect specific devices (classified profiles) and groups of devices (aggregate profiles) against SYN, UDP, ICMP, ICMPv6, and Other IP flood attacks.

upvoted 3 times

  **shane** 3 years, 6 months ago



correct C

upvoted 1 times

  **Sarbi** 3 years, 9 months ago

Anser c

upvoted 1 times

  **lol1000** 3 years, 10 months ago

Answer c

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-web-interface-help/network/network-network-profiles/network-network-profiles-zone-protection/reconnaissance-protection.html#ida0512c75-ed54-4b31-8d2c-9f459466d4d2>

upvoted 1 times

▣ 👤 **UmaShankar** 3 years, 10 months ago

Correct answer is c
upvoted 1 times

▣ 👤 **kerberos** 4 years ago

Zone Protection Profiles defend the zone at the ingress zone edge against reconnaissance port scan and host sweep attacks, IP packet-based attacks, non-IP protocol attacks, and flood attacks by limiting the number of connections per second (CPS) of different packet types.
upvoted 2 times

▣ 👤 **KAACK** 4 years, 1 month ago

Correct: C
upvoted 2 times

▣ 👤 **ChiaPet75** 4 years, 2 months ago

Correct: C
Reconnaissance Protection includes:
TCP Port Scan
UDP Port Scan
Host Sweep
upvoted 2 times

▣ 👤 **asmaam** 4 years, 5 months ago

Correct ans = C
upvoted 2 times

▣ 👤 **khalmrj** 4 years, 6 months ago

correct C
upvoted 2 times

▣ 👤 **Mello** 4 years, 10 months ago

The Correct answer is C

<https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/network/network-network-profiles-zone-protection.html>

upvoted 4 times

Which CLI command can be used to export the tcpdump capture?

- A. scp export tcpdump from mgmt.pcap to < username@host:path>
- B. scp extract mgmt-pcap from mgmt.pcap to < username@host:path>
- C. scp export mgmt-pcap from mgmt.pcap to < username@host:path>
- D. download mgmt-pcap

Correct Answer: C

Reference:

<https://live.paloaltonetworks.com/t5/Management-Articles/How-To-Packet-Capture-tcpdump-On-Management-Interface/ta-p/55415>

  **rajputparveen** Highly Voted 4 years, 2 months ago

C is the correct one
upvoted 8 times

  **duckduckgoo** 1 year, 5 months ago

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000wkpQCAQ&lang=en_US%E2%80%A9
upvoted 1 times

  **Prutser2** Highly Voted 3 years, 2 months ago

u supposed to know this stuff of the top of your head, seriously
upvoted 5 times


  **GivemeMoney** 2 years, 7 months ago

yep, bullshit right??
upvoted 1 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: C

C is correct
upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: C

C is the correct one
upvoted 2 times

  **NHANTON** 2 years, 7 months ago

it is very confused . because export tcpdump in question, but mgmt-cap in answer.
upvoted 2 times

  **myname_1** 1 year, 8 months ago

tcpdump is a command, mgmt-pcap is the type of dump captured and mgmt.pcap is the file outputted by tcpdump
upvoted 1 times

  **UmaShankar** 3 years, 10 months ago

C is the correct one
upvoted 1 times

An administrator has configured the Palo Alto Networks NGFW's management interface to connect to the internet through a dedicated path that does not traverse back through the NGFW itself.

Which configuration setting or step will allow the firewall to get automatic application signature updates?

- A. A scheduler will need to be configured for application signatures.
- B. A Security policy rule will need to be configured to allow the update requests from the firewall to the update servers.
- C. A Threat Prevention license will need to be installed.
- D. A service route will need to be configured.

Correct Answer: A

  **Edu147** Highly Voted 5 years, 1 month ago

Correct Answer: A

You don't need a service route. Those are only used when you are using an interface OTHER THAN the MGMT interface.

upvoted 26 times

  **PacketFairy** 3 years, 9 months ago

It clearly says the Mgmt interface has internet access, not through the firewall. The only thing to configure is the schedule for all dynamic updates.

upvoted 9 times

  **hcir** Most Recent 2 months, 3 weeks ago

for Application updates, you do not need a Threat Prevention license. C would have been the answer if updates for app and content were mentioned. So the only sensible answer is A

upvoted 1 times

  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: A

A : new document[<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/device/device-dynamic-updates>]

upvoted 2 times

  **JMIB** 2 years ago

A

You don't need to configure a service route for management interfaces by default. But you need to create a scheduler for automatic updates

upvoted 1 times

  **Pretorian** 2 years, 1 month ago

One more example (like most of the PCNSX questions) of a malicious PANW test question. The answer seems to be "A" but it's tricky AF

upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: A

A

You don't need to configure a service route for management interfaces by default. But you need to create a scheduler for automatic updates

upvoted 2 times

  **Abu_Muhammad** 2 years, 4 months ago

Selected Answer: A

As mentioned by the other guys , service route is needed only if you will use a non-mgmt interface

upvoted 2 times

  **tururu1496** 2 years, 6 months ago

Answer: A

upvoted 1 times

  **NHANTON** 2 years, 7 months ago



A is correct. this is a good confusing question.

upvoted 3 times

  **joaohbert** 2 years, 11 months ago



A is correct = <https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-web-interface-help/device/device-dynamic-updates.html#idef12a8e2-9abb-48cd-851f-77b13eca01bb>

upvoted 2 times

  **Zabol** 3 years, 2 months ago

A is Correct

upvoted 1 times

  **YasserSaied** 3 years, 2 months ago



A -- question has bad wording and unclear

upvoted 2 times

  **yogininangpal** 3 years, 4 months ago

A is the correct answer as management interface has dedicated internet access!

upvoted 1 times

  **evdw** 3 years, 4 months ago

Correct answer : A

upvoted 1 times

  **trashboat** 3 years, 4 months ago


A is the correct answer, see other comments. Updates will not happen automatically unless you schedule them:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-web-interface-help/panorama-web-interface/panorama-device-deployment/schedule-dynamic-content-updates.html>

Also note that there are recommended update intervals (this probably won't be on the test):

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClaECAS>

upvoted 2 times

  **rocioha** 3 years, 4 months ago

A is the right answer, you don't need a service route here. and the others does not have any sense

upvoted 1 times

Which three options are supported in HA Lite? (Choose three.)

- A. Virtual link
- B. Active/passive deployment
- C. Synchronization of IPsec security associations
- D. Configuration synchronization
- E. Session synchronization

Correct Answer: BCD

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-high-availability/ha-lite>

  **Silent_Sanctuary** Highly Voted 4 years, 3 months ago

Correct Answer B C & D

HA Lite is an active/passive deployment that provides configuration synchronization and some run-time data synchronization such as IPsec security associations. It does not support session synchronization (HA2), and therefore does not offer stateful failover.

upvoted 21 times

  **eyelasers1** 2 years, 6 months ago

Note that HA Lite is not present in PAN 10: Compare 8.1 and 10 docs here: <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/high-availability/ha-concepts/ha-modes.html>

upvoted 2 times

  **duckduckgoo** 1 year, 5 months ago

New link

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIUzCAK>



upvoted 1 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: BCD

B, C and D correct

upvoted 1 times

  **Sarbi** 1 year, 8 months ago



ACD is 100 % correct answer

upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

No its BCD. <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIUzCAK>

upvoted 1 times

  **secdaddy** 1 year, 11 months ago

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIUzCAK>

upvoted 1 times

  **shinichi_88** 2 years, 7 months ago

b c d correct

upvoted 1 times

  **aadach** 3 years, 5 months ago



once again: AP AA, config and session sync I've just checked it

upvoted 1 times

  **aadach** 3 years, 5 months ago

See that v10 PANOS gives: A/P, Enable Config Sync, Enable Session Synchronization

upvoted 1 times

  **mmed** 3 years, 5 months ago

BCD

HA-Lite offers the following capabilities:

A/P High Availability without session sync

Failover of IPSec Tunnels (sessions must be re-established)

DHCP Lease information

PPPoE lease information

Configuration sync
Layer 3 forwarding tables
upvoted 4 times

lol1000 3 years, 10 months ago

b, c, d
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIUzCAK>
upvoted 2 times

cybermate 4 years, 3 months ago

BCD are the correct answers
The PA-200 (a discontinued model) firewall supports HA Lite only. HA Lite is an active/passive deployment that provides configuration synchronization and some run-time data synchronization such as IPsec security associations. It does not support session synchronization (HA2), and therefore does not offer stateful failover.
upvoted 4 times

Question #64

Topic 1

Which CLI command enables an administrator to view details about the firewall including uptime, PAN-OS® version, and serial number?

- A. debug system details
- B. show session info
- C. show system info
- D. show system details

Correct Answer: C

Reference:

<https://live.paloaltonetworks.com/t5/Learning-Articles/Quick-Reference-Guide-Helpful-Commands/ta-p/56511>

lol1000 3 years, 10 months ago

c
checked on my appliance
upvoted 6 times

dev46 4 years, 2 months ago

C is correct

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIZuCAK>
upvoted 5 times

Marshpillowz 7 months, 2 weeks ago

Selected Answer: C

C is correct
upvoted 1 times

JMIB 2 years ago

Correct Answer: C
upvoted 1 times

fireb 2 years, 3 months ago

Correct option: C
upvoted 1 times

confusion 2 years, 6 months ago

Selected Answer: C

C checked in LAB
upvoted 1 times

During the packet flow process, which two processes are performed in application identification? (Choose two.)

- A. Pattern based application identification
- B. Application override policy match
- C. Application changed from content inspection
- D. Session application identified

Correct Answer: AB

[-] **tester12** Highly Voted 4 years, 11 months ago

Should be A and B

<http://live.paloaltonetworks.com//t5/image/serverpage/image-id/12862i950F549C7D4E6309>

upvoted 34 times

[-] **asmaam** Highly Voted 4 years, 5 months ago

Correct ans = AB

upvoted 9 times

[-] **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: AB

A and B are correct

upvoted 1 times

[-] **Pakawat** 2 years, 2 months ago

Correct answer are A, B

upvoted 2 times

[-] **UFanat** 2 years, 2 months ago

Selected Answer: AB

First and second step during application identification:

Application override policy match

Pattern based application identification

upvoted 1 times

[-] **Dimida** 2 years, 5 months ago

Selected Answer: AB

A,B right

upvoted 2 times

[-] **AbuHussain** 2 years, 5 months ago

Selected Answer: AB

Should be A and B

upvoted 3 times

[-] **tururu1496** 2 years, 6 months ago

Answer: A,B

upvoted 1 times

[-] **unknid** 2 years, 7 months ago

Selected Answer: AB

A+B = Identified by behavioral heuristics

upvoted 3 times

[-] **YasserSaied** 3 years, 2 months ago

A & B --- A: Signature Match, B: App Override

upvoted 2 times

[-] **yogininangpal** 3 years, 4 months ago

The obvious answer is AB and a nuanced answer is AC. The packet flow shows clearly AB but really in application detection the decoders are used and the tunneled applications are identified so there is kind of overlap in real application identification process in the packet flow. One thing to remember is do not pick nuanced answers only pick the obvious answers in the exam!!

upvoted 3 times

[-] **evdw** 3 years, 4 months ago

Correct Answer: A, B

upvoted 1 times


  **trashboat** 3 years, 4 months ago

I think this is a bad question, because the PAN-OS Packet Flow Sequence says that during Application Identification, the application session is identified, but it also says pattern-based application identification is used. So really the answer could be A&B or B&D.

See both the packet flow diagram, as well as Section 5 ("...the firewall identifies the session application...")

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVHCA0>

upvoted 1 times

  **Adamabdi** 3 years, 5 months ago

A and B are correct .


<http://live.paloaltonetworks.com//t5/image/serverpage/image-id/12862i950F549C7D4E6309>

upvoted 2 times

  **aadach** 3 years, 5 months ago



only BD !

upvoted 1 times

  **hpbdcdb** 3 years, 9 months ago

A and B

upvoted 4 times

  **Ripu** 4 years, 2 months ago

Correct Answer:A,B

upvoted 6 times

Which tool provides an administrator the ability to see trends in traffic over periods of time, such as threats detected in the last 30 days?

- A. Session Browser
- B. Application Command Center
- C. TCP Dump
- D. Packet Capture

Correct Answer: B

Reference:

<https://live.paloaltonetworks.com/t5/Management-Articles/Tips-and-Tricks-How-to-Use-the-Application-Command-Center-ACC/ta-p/67342>

  **dev46** Highly Voted 4 years, 2 months ago

B is correct

B

The Application Command Center (ACC) page visually depicts trends and a historic view of traffic on your network. It displays the overall risk level for all network traffic, the risk levels and number of threats detected for the most active and highest-risk applications on your network, and the number of threats detected from the busiest application categories and from all applications at each risk level. The ACC can be viewed for the past hour, day, week, month, or any custom-defined time frame.

upvoted 9 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

  **JMIB** 2 years ago

Correct Answer: B



upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: B

ACC is designed for it



upvoted 1 times

  **confusion** 2 years, 6 months ago

Selected Answer: B



ACC can provide thread reporting

upvoted 2 times

  **lol1000** 3 years, 10 months ago

b correct

upvoted 4 times

  **Dexy** 4 years, 2 months ago

This should be B

upvoted 4 times

The certificate information displayed in the following image is for which type of certificate?

Certificate information

Name: demo-decrypt

Subject: /CN=sub.domain.local

Issuer: /CN=demo.local

Not Valid Before: Jul 23 16:52:26 2020 GMT

Not Valid After: Jul 23 16:52:26 2020 GMT

Algorithm: RSA

Certificate Authority

Forward Trust Certificate

Forward Untrust Certificate

Trusted Root CA

Buttons: Revoke, OK, Cancel

- A. Forward Trust certificate
- B. Self-Signed Root CA certificate
- C. Web Server certificate
- D. Public CA signed certificate

Correct Answer: B

kike71 Highly Voted 3 years, 2 months ago

B is correct
A CA self-signed only can be a RootCA. Issuer CN and Certificate CN are equal
upvoted 11 times

Marshpillowz Most Recent 7 months, 2 weeks ago

Selected Answer: B

Answer is B
upvoted 1 times

JRKhan 7 months, 4 weeks ago

Selected Answer: B

The question and answers do not match but i think the expected answer is B. Its actually an Intermediate certificate capable of signing other certificates. It is not self signed or a root cert as the issuer field mentions the root cert that signed this cert.
upvoted 2 times

DatITGuyTho1337 8 months, 3 weeks ago

People that voted for "A" should have looked at the diagram where the option for Forward Trust Certificate remained unchecked.
upvoted 2 times

snoop88 9 months, 4 weeks ago

Selected Answer: C

The expiry and subject
upvoted 2 times

Micutzu 10 months, 3 weeks ago

Selected Answer: B

The most close answer it's B. Actually the information displayed shows an Self-Signed Intermediate Root CA.
upvoted 1 times

[Removed] 12 months ago

Selected Answer: B

Not a forward trust because box not checked.
Answer is B CN .local
upvoted 1 times

[-]  **kewokil120** 1 year, 5 months ago

Selected Answer: B

B is correct.
upvoted 2 times

[-]  **Pochex** 1 year, 6 months ago

From my perspective there is no correct answer:

A is not correct since 'Forward Trust certificate' option is not selected
B is wrong because subject and issuer are not the same so this is not a self-signed cert
C would not be right because this is a firewall cert and not a cert coming from a Web Server
D is not correct, CA signed cert should a

I've seen the same question with another screenshot in which the issuer and the subject contain the same IP address, in such case the correct answer would be A...

upvoted 2 times

[-]  **Knowledge33** 1 year, 3 months ago

This is the question you are talking about:
<https://vceguide.com/which-type-of-certificate/>


The screenshot here is totally false. They paste the wrong picture.

upvoted 2 times

[-]  **Knowledge33** 1 year, 3 months ago

You're wrong. In this case you mentioned, the response would be B (self-signed CA).

upvoted 1 times

[-]  **Pochex** 1 year, 6 months ago

I meant, D is not correct, CA signed cert would have the same issuer and subject

upvoted 1 times

[-]  **Frightened_Acrobat** 1 year, 6 months ago

B.
You can rule out the others.
Forward Trust certificate is not checked.
Not a server certificate.
Not a Public signed certificate.
The screenshot matches what a self-signed certificate would look like. That only leaves B.
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cla8CAC>
upvoted 1 times

[-]  **thissiteisgreat** 1 year, 8 months ago

Selected Answer: A

Answer is A. Cannot be a self-signed certificate as suggested by sTryogetOn

upvoted 1 times

[-]  **vpnmcfrcwoljkmegdh** 1 year, 8 months ago

Selected Answer: A

A is correct
upvoted 1 times

[-]  **Kuronekosama** 1 year, 10 months ago

Selected Answer: B

Forward trust box not selected.

Answer is B

upvoted 3 times

[-]  **sTryogetOn** 1 year, 11 months ago

Selected Answer: A

A is correct.
The displayed certificate clearly shows it has a different CN than the Issuer, which means it is NOT self-signed. The displayed certificate is a Sub/Intermediate CA cert, which means it can sign certificates, which is a requirement for the Forward Trust Certificate.

upvoted 2 times

[-]  **nekkrokvlt** 2 years ago


But this is not a root CA, Issuer and Subject are not the same. I think correct answer would be CA Signed CA, but not from public CA, so correct answer seems not present

upvoted 2 times

[-]  **JMIB** 2 years ago

Correct Answer: B

upvoted 2 times

  **Gabuu** 2 years, 1 month ago

b is correct

upvoted 2 times

Which three steps will reduce the CPU utilization on the management plane? (Choose three.)

- A. Disable SNMP on the management interface.
- B. Application override of SSL application.
- C. Disable logging at session start in Security policies.
- D. Disable predefined reports.
- E. Reduce the traffic being decrypted by the firewall.

Correct Answer: ACD

  **Edu147** Highly Voted 5 years, 1 month ago

Correct A,C,D

B and E are a data plane function.
upvoted 25 times

  **tester12** 4 years, 11 months ago

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleLCAS>
upvoted 6 times

  **asmaam** Highly Voted 4 years, 5 months ago

Correct ans = ACD
upvoted 7 times



  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: ACD

A, C and D are correct.
upvoted 1 times

  **JMIB** 2 years ago



Correct Answer: ACD (Only Disable)
A. Disable
C. Disable
D. Disable
upvoted 2 times

  **evdw** 3 years, 4 months ago



Correct Answer : A, C, D
upvoted 3 times

  **TIDUARTE** 3 years, 5 months ago

Work experience. CDE
upvoted 2 times

  **Raikin** 3 years, 4 months ago

E is data plane
upvoted 1 times

  **vj77** 3 years, 4 months ago

How do you encrypt/decrypt data on mgmt plane?
upvoted 4 times

  **Rasta2** 3 years, 7 months ago

Answers should be A,C,D.



B is out of discussion;

I don't think it's E because from the study guide: "Every Palo Alto Networks firewall assigns a minimum of these functions to the management plane:

- Configuration management
- Logging
- Reporting functions
- User-ID agent process
- Route updates

- Signature Match Processor:
- All Content-ID and App-ID services
- Security Processors:



- Session management
 - Encryption and decryption <====Data Plane
 - Compression and decompression
 - Policy enforcement
 - Network Processor:
 - Route
 - ARP
 - MAC lookup
 - QoS
 - NAT
 - Flow control"
- upvoted 4 times

  **ochc** 3 years, 9 months ago

CDE - "PA-32xx and above (so All 5k, 7k etc) does SSL decryption in hardware. PA-2xx, PA-8xx and PA30xx are software. This means your MP CPU usage is expected." ref
https://www.reddit.com/r/paloaltonetworks/comments/8s9gay/ssl_decryption_causing_high_management_plane_cpu/e0xuo5i/
upvoted 1 times

  **hpbdc** 3 years, 9 months ago

correct is: CDE
upvoted 1 times

  **lol1000** 3 years, 10 months ago

ACD correct
upvoted 1 times

  **kamikaze** 3 years, 11 months ago

i think the correct answer is CDE,

because in this article :

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleLCAS>



there is only mention to disable logging for snmp, not to disable SNMP. imagine if you disable SNMP on management interface, how you get snmp from HA device ? it will never happen on secondary firewall.

and this article:

<https://live.paloaltonetworks.com/t5/general-topics/ssl-decryption-and-load-on-management-plane/td-p/236408>

tells that decryption will using management plan, and will increase load of management plan.

upvoted 3 times

  **KA** 4 years, 1 month ago

ACD

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleLCAS>

upvoted 4 times

  **Ahmad_Zahran** 4 years, 4 months ago

Correct A,C,D

upvoted 5 times

Which feature must you configure to prevent users from accidentally submitting their corporate credentials to a phishing website?

- A. URL Filtering profile
- B. Zone Protection profile
- C. Anti-Spyware profile
- D. Vulnerability Protection profile

Correct Answer: A

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/threat-prevention/prevent-credential-phishing>

  **_taintsmasher** Highly Voted 4 years, 4 months ago

A, updated reference

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/prevent-credential-phishing/set-up-credential-phishing-prevention>

upvoted 13 times

  **MarkyMarc** Highly Voted 3 years, 6 months ago

A is correct. Phishing attack prevention extends the URL filtering capabilities to actively detect targeted credential phishing attacks through a cloud-based analytics service as well as through heuristics on the device itself.


upvoted 7 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: A

A is the correct answer



upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: A

A. new document [<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/url-filtering/prevent-credential-phishing/set-up-credential-phishing-prevention>]

upvoted 2 times

  **lol1000** 3 years, 10 months ago

A is correct

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/url-filtering/prevent-credential-phishing/set-up-credential-phishing-prevention.html>

upvoted 6 times

  **Isolated** 4 years, 2 months ago

tHNX bRO

upvoted 2 times

How can a candidate or running configuration be copied to a host external from Panorama?

- A. Commit a running configuration.
- B. Save a configuration snapshot.
- C. Save a candidate configuration.
- D. Export a named configuration snapshot.

Correct Answer: D

Reference:

https://www.paloaltonetworks.com/documentation/71/panorama/panorama_adminguide/administer-panorama/back-up-panorama-and-firewall-configurations

  **dev46** Highly Voted 4 years, 2 months ago

D is correct

<https://docs.paloaltonetworks.com/panorama/7-1/panorama-admin/administer-panorama/back-up-panorama-and-firewall-configurations>
upvoted 8 times

  **lol1000** Highly Voted 3 years, 10 months ago

d is correct



<https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/administer-panorama/manage-panorama-and-firewall-configuration-backups/save-and-export-panorama-and-firewall-configurations.html>
upvoted 5 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

Selected Answer: D

D. 100 percent!

upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: D


D. update reference[<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/administer-panorama/manage-panorama-and-firewall-configuration-backups/save-and-export-panorama-and-firewall-configurations>]

upvoted 2 times

  **trashboat** 3 years, 4 months ago

D - you have to first save the config, then to get it on another device you must export it, then import it on the other device locally

upvoted 4 times

  **rocioha** 3 years, 5 months ago

D because you must to save and then export

upvoted 2 times

If an administrator does not possess a website's certificate, which SSL decryption mode will allow the Palo Alto Networks NGFW to inspect traffic when users browse to HTTP(S) websites?

- A. SSL Forward Proxy
- B. SSL Inbound Inspection
- C. SSL Reverse Proxy
- D. SSL Outbound Inspection

Correct Answer: A

  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: A

Answer is A

upvoted 1 times

  **Woody** 1 year, 8 months ago

"If an administrator does not possess a website's certificate, which SSL decryption mode will allow the Palo Alto Networks NGFW to INSPECT traffic when users browse to HTTP(S) websites?"

Should that not be B? SSL Forward Proxy mode does not inspect the SSL traffic but Inbound Inspection Decryption Mode does!

upvoted 2 times

  **Knowledge33** 1 year, 3 months ago

I though like you, but it's not correct. Don't matter about "If an administrator certificate". Only focus to the rest of the sentence "which SSL websites?" You'll see the answer is evident.

upvoted 1 times

  **myname_1** 1 year, 8 months ago

I think the key here it says users, not external users. If it said external users, we would be looking at ssl inbound most likely.

upvoted 2 times

  **secdaddy** 2 years, 1 month ago

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIV8CAK>

upvoted 3 times

  **Gabuu** 2 years, 1 month ago

Selected Answer: A

its an outbound traffic so you will need SSL Forward proxy

upvoted 4 times

  **UFanat** 2 years, 2 months ago

Selected Answer: A

SSL inbound inspection can be used if you possess a website's certificate, otherwise - only SSL Forward Proxy

upvoted 4 times

  **AbuHussain** 2 years, 5 months ago

Selected Answer: A

Answer: A

upvoted 3 times

  **tururu1496** 2 years, 6 months ago

Answer: A



upvoted 3 times

  **GivemeMoney** 2 years, 7 months ago

Selected Answer: A

It's A. SSL Forward Proxy



upvoted 3 times

  **zyizi** 2 years, 8 months ago

Selected Answer: A

Here, it's A

upvoted 4 times

  **Breyarg** 2 years, 8 months ago

no the answer is A. forward proxy. the direction is outbound not inbound.
upvoted 2 times

An administrator sees several inbound sessions identified as unknown-tcp in the Traffic logs. The administrator determines that these sessions are from external users accessing the company's proprietary accounting application. The administrator wants to reliably identify this traffic as their accounting application and to scan this traffic for threats.

Which option would achieve this result?

- A. Create a custom App-ID and enable scanning on the advanced tab.
- B. Create an Application Override policy.
- C. Create a custom App-ID and use the "ordered conditions" check box.
- D. Create an Application Override policy and a custom threat signature for the application.

Correct Answer: A

  **trashboat** Highly Voted 3 years, 4 months ago

A is the correct answer:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/app-id/manage-custom-or-unknown-applications.html>



upvoted 6 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: A

A is correct


upvoted 1 times

  **sov4** 1 year, 1 month ago

Selected Answer: A

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRoCAK>

upvoted 1 times

  **drpcc** 1 year, 1 month ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/app-id/manage-custom-or-unknown-applications.html>
"create a custom application and define an application override policy"

upvoted 1 times



  **Xuzi** 10 months ago

D option is not saying "custom" but - Create an Application Override policy.

Create a Custom Application with a signature and attach it to a security policy, or create a custom application and define an application override policy



<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/app-id/manage-custom-or-unknown-applications>

upvoted 1 times

  **Sarbi** 1 year, 8 months ago



It is B. Once you enable application override it will not go beyond layer 4.

upvoted 2 times

  **javim** 1 year, 7 months ago

I agree

upvoted 1 times

  **sujss** 1 year, 5 months ago

Then how would this be accomplished ?

"and to scan this traffic for threats."



upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: A

Application Override policy disables scan for threats

upvoted 2 times

  **Gngogh** 1 year, 9 months ago

it depends if you choose a parent app or not


upvoted 1 times

  **datz** 2 years, 3 months ago



Selected Answer: A

Correct a


<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRoCAK>
upvoted 1 times

  **hpbdc** 3 years, 9 months ago

absolutely A. take note of "reliably identify" here - which excludes B.
upvoted 4 times

  **ameeeeen** 3 years, 7 months ago

True, it's also said ' to scan this traffic for threats' which exludes B too
upvoted 2 times

  **MS_NW** 4 years, 1 month ago

Looks like A
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRoCAK>
upvoted 4 times

The administrator has enabled BGP on a virtual router on the Palo Alto Networks NGFW, but new routes do not seem to be populating the virtual router.

Which two options would help the administrator troubleshoot this issue? (Choose two.)

- A. View the System logs and look for the error messages about BGP.
- B. Perform a traffic pcap on the NGFW to see any BGP problems.
- C. View the Runtime Stats and look for problems with BGP configuration.
- D. View the ACC tab to isolate routing issues.

Correct Answer: BC

  **ChiaPet75** Highly Voted 4 years, 2 months ago

Correct: B,C

=====

PAN-EDU-311 Advanced Troubleshooting Dynamic Routing module

"Confirm virtual router runtime status on the active firewall, go to the Network > Virtual Router screen and click on More Runtime Stats"

=====

<https://live.paloaltonetworks.com/t5/general-topics/bgp-traffic-pcap/td-p/237407>

For troubleshooting purposes it may be necessary to collect the PCAPs of the OSPF and BGP traffic that the Palo Alto Networks device is processing. The quickest way to perform troubleshooting is through the CLI.

To start the BGP capture, use the following CLI command:

```
> debug routing pcap bgp on
```

upvoted 25 times

  **hcir** 2 months, 3 weeks ago

debug routing pcap bgp on is not a traffic pcap, but a management plane pcap

upvoted 1 times

  **Breyarg** 2 years, 8 months ago


agreed. i have had to TS this a good few times and only these options actually seem relevant to real life.

upvoted 1 times

  **Edu147** Highly Voted 5 years, 1 month ago

Correct A,C

upvoted 9 times

  **tester12** 4 years, 11 months ago

Why is not B instead of A ?

upvoted 1 times

  **jonboy22** 2 years, 2 months ago

Probably because B requires more practical legwork than A or C do.

upvoted 1 times

  **kambata** Most Recent 2 months ago

Selected Answer: AC

Idiotic question, but of course you will check the logs before doing a capture ... B is also valid, but I would go with A and C

upvoted 1 times

  **hcir** 2 months, 3 weeks ago

A and B. It cannot be C because in the runtime stats, you do not look for configuration issues.

upvoted 2 times

  **123XYZT** 4 months, 3 weeks ago

I think is A and B

upvoted 2 times

  **techplus** 11 months ago

Selected Answer: AC

A & C are the correct answer

upvoted 2 times

sov4 1 year, 1 month ago

Selected Answer: AC

I would say AC. The question is very similar to the next on (#74) concerning OSPF. They're both routing protocols so it's reasonable to begin basic troubleshooting the same way -- look at the system logs and stats.

upvoted 2 times

playthegamewithme 1 year, 2 months ago

It cant be A because, the system logs doesn't generate logs when it comes to traffic, Ive been through the system logs loads of times and never seen BGP traffic errors being logged.

B and C looks more relevant

upvoted 1 times

hcir 2 months, 3 weeks ago

system logs generates events related to bgp

upvoted 1 times

DenskyDen 1 year, 6 months ago

Selected Answer: BC

Tested this.

upvoted 1 times

lildevil 1 year, 5 months ago

And your results?

upvoted 1 times

hdrnzenlaoroljol 1 year, 6 months ago

Selected Answer: BC

B and C

upvoted 1 times

mic_mic 1 year, 8 months ago

Which two options would help the administrator troubleshoot this issue? Can it be A and B?

When I view the Runtime Stats, can I troubleshoot? or only see the stats?

When I look into the sytem log I see info why not onlu stats (just think out loud)

upvoted 2 times

TAKUM1y 1 year, 11 months ago

Selected Answer: BC

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/network/network-virtual-routers/more-runtime-stats-for-a-virtual-router#id37f2aaf9-bb39-40e8-a838-33f22ccbc05e>

upvoted 2 times

UFanat 2 years, 2 months ago

Selected Answer: BC

C is correct 100%

Between A and B - i choose B:

> debug routing pcap bgp on

this command is designed for BGP troubleshooting as asked in the question

upvoted 1 times

datz 2 years, 3 months ago

so C is correct.

Second answer = Could be A as inside system logs we can filter is based on BGP and see what errors we get. PCAP could possibly valid too...

Also if we are saying no new routes are being populated to vRouter, what is the point of checking runtime logs :/ zzz

upvoted 1 times

asdasd123123iu 2 years, 4 months ago

I think that A and C are correct. We can check BGP events on System tab and Virtual Router Runtime Status. Capturing traffic is required when we must check if connectivity between peers works correctly.

upvoted 2 times

Joey456 3 years, 3 months ago

'Which two options would help...' Not conclusively identify.

Troubleshooting best practices dictate you start with the least involved measures. Of the options, performing a PCAP is the most involved.

A, B.

upvoted 4 times

trashboat 3 years, 4 months ago

B is definitely one of the correct options. BGP debug pcap commands will show by far the most detail when troubleshooting BGP.

However, A and C could both be correct. You can view status of BGP in the Runtime Stats section of the Virtual Router and this could tell you if BGP is configured incorrectly (but BGP not establishing isn't necessarily an indicator there is a misconfiguration locally); however this is not where BGP is configured (you have to open/edit the actual VR to configure BGP.)

For that reason I think A would be the other correct answer, as you can view BGP events in System logs with this filter: (subtype eq routing) and (description contains 'BGP'), which is more useful for actual troubleshooting than just seeing current status.

upvoted 7 times

  **mohr22** 1 year, 6 months ago

A and B is correct. View will give same information which is already has been known in question.

upvoted 1 times

An administrator has enabled OSPF on a virtual router on the NGFW. OSPF is not adding new routes to the virtual router. Which two options enable the administrator to troubleshoot this issue? (Choose two.)

- A. View Runtime Stats in the virtual router.
- B. View System logs.
- C. Add a redistribution profile to forward as BGP updates.
- D. Perform a traffic pcap at the routing stage.

Correct Answer: AB

  **rammsdoct** Highly Voted 4 years, 2 months ago

For me as more native network-engineer, I will always check/debug any routing protocol, so at first glance I will choose A-B but as per PA procedure seems to be A-D, check below.

<https://live.paloaltonetworks.com/t5/general-topics/bgp-traffic-pcap/td-p/237407>

For troubleshooting purposes it may be necessary to collect the PCAPs of the OSPF and BGP traffic that the Palo Alto Networks device is processing. The quickest way to perform troubleshooting is through the CLI.

Enjoy

upvoted 20 times

  **Breyarg** 2 years, 8 months ago

i would agree but theres no "routing stage" when it comes to PCAPS. theres the following only:

FW
Drop
Receive
Transmit

so must be AB.

upvoted 7 times

  **[Removed]** 1 year, 4 months ago

A and D should be correct

upvoted 1 times

  **[Removed]** 1 year, 4 months ago

A nd B, I read again opcion D and it says "at routing stage" and you cant take a packet caputer in that "stage"

upvoted 2 times

  **Edu147** Highly Voted 5 years, 1 month ago

Correct A,B

upvoted 13 times

  **Eluis007** Most Recent 5 months ago

Selected Answer: AD

rammsdoct correct



upvoted 1 times

  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: AB

A and B correct

upvoted 1 times

  **sov4** 1 year, 1 month ago

Selected Answer: AB

AB. D doesnt make sense. There isnt a routing stage.

upvoted 1 times

  **notsosavyv** 1 year, 4 months ago

Selected Answer: AB

D is not valid due to the fact there is no "routing stage", correct answers are A & B

upvoted 1 times

  **hdrnzenlaoroljol** 1 year, 6 months ago

Selected Answer: AB

A and B

upvoted 1 times

mohr22 1 year, 6 months ago

B & D is correct .

B to see error logs related to ospfv3

D to capture ospf routing related logs .

> debug routing pcap

> all

> bgp

> igmp

> ospf

> ospfv3

> pim

> rip

There is not view run stat option for ospf.

upvoted 3 times

JMIB 2 years ago

Correct Answer: AB (Only view)

A. View

B. View

upvoted 1 times

Scryptre 2 years, 9 months ago

but isnt this question the same as #73, just different protocol?

#73 b) perform traffic pcap and c) view runtime stats

#74 a) view Runtime Stats and d) perform traffic pcap

upvoted 9 times

travelmrj 3 years, 2 months ago

A and B

upvoted 2 times

trashboat 3 years, 4 months ago

A & B are correct.

C doesn't apply and D is not a thing in PAN-OS.

However I still think that Runtime Information is not the best for troubleshooting - CLI debug commands will work best, or even System Logs will show more actual event information for troubleshooting, use this filter:

(subtype eq routing) and (description contains 'OSPF')

upvoted 2 times

aadach 3 years, 5 months ago

A - OK, D - not, cos packet_capture with "routing stage" doesn't exist, so, A B is correct

upvoted 2 times

KAAC 4 years, 1 month ago

A,B is correct

upvoted 3 times

MS_NW 4 years, 1 month ago

Agree with cthd , A and D

upvoted 3 times

KAM2020 4 years, 1 month ago

There is no routing stage, it's "forwarding" stage

upvoted 2 times

cthd 4 years, 2 months ago

The question is asking about OSPF, and the C is about BGP, that makes C is incorrect answer...Should be A and D

upvoted 4 times

Raikin 3 years, 4 months ago

There is no routing stage in pcap...

upvoted 1 times

yjquiver 4 years, 4 months ago

correct answer is AB

upvoted 4 times

Which three firewall states are valid? (Choose three.)

- A. Active
- B. Functional
- C. Pending
- D. Passive
- E. Suspended

Correct Answer: ADE

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-firewall-states>

  **lol1000** Highly Voted 3 years, 10 months ago

ade

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/high-availability/ha-firewall-states.html>


upvoted 10 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: ADE

A, D and E correct

upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

ADE. 100 percent.

upvoted 1 times

  **Kjohnsting** 1 year, 9 months ago

Suspended is when you force a fw to passive.

upvoted 1 times

  **c001mud** 1 year, 11 months ago

Selected Answer: ADE

ade for sure

upvoted 3 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: ADE

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-firewall-states#id2ee5562a-9bc8-42b6-9c77-2cc496a112fc>

upvoted 1 times

  **UFanat** 2 years, 2 months ago

Active (A)

Passive (D)

Suspended (E)

Non-Functional

Initial

Tentative

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/high-availability/ha-firewall-states>

upvoted 3 times

  **confusion** 2 years, 6 months ago

Selected Answer: ADE

ADE 100%



upvoted 2 times

  **thefiresays** 2 years, 12 months ago

ADE

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/high-availability/ha-firewall-states.html>

upvoted 3 times

  **evdw** 3 years, 4 months ago

Correct answer: A, D, E

upvoted 2 times

[-] 👤 **lucaboban** 3 years, 5 months ago

Correct answer is: ADE

upvoted 3 times

[-] 👤 **PacketFairy** 3 years, 9 months ago

A, C, E - One of the operations is to "suspend" a firewall. Often used to force an HA event. Also, if HA goes crazy and flaps back and forth, after 3 flaps the active firewall will go into "suspend" state. A hard failure is easier to diagnose than a constantly changing HA state. If HA is enabled, these are the states you will see on the dashboard. Everything else is a diagnostic mode or part of the boot sequence.

upvoted 4 times

[-] 👤 **frodo1791** 3 years, 4 months ago

Pending is not a valid HA Cluster state, it makes options B and C incorrect.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/ha-firewall-states>

upvoted 2 times

[-] 👤 **confusion** 2 years, 5 months ago

ADE, not ACE

upvoted 1 times

[-] 👤 **CyberRasta** 2 years, 11 months ago

Why C? You said it yourself "after 3 flaps the active firewall will go into "suspend" state -----> Suspended STATE

upvoted 1 times

[-] 👤 **zhawk7661** 4 years, 1 month ago

ANSWER: A,D,E

upvoted 4 times

Which virtual router feature determines if a specific destination IP address is reachable?

- A. Heartbeat Monitoring
- B. Failover
- C. Path Monitoring
- D. Ping-Path

Correct Answer: C

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/policy-based-forwarding/pbf/path-monitoring-for-pbf>

  **phannyalto** Highly Voted 4 years, 4 months ago

C is correct
upvoted 8 times

  **sethjam** Highly Voted 4 years, 2 months ago

Ans. C.

Path monitoring allows you to verify connectivity to an IP address so that the firewall can direct traffic through an alternate route, when needed.

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/pbf>

upvoted 6 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: C

C is correct
upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/policy-based-forwarding/pbf/path-monitoring-for-pbf>

upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: C

path mon
upvoted 2 times

  **confusion** 2 years, 6 months ago

Selected Answer: C

C. Path monitoring is used to determine if remote IP is reachable.

upvoted 2 times

  **Narendragpt** 3 years, 5 months ago

C is correct - <https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/policy/policy-based-forwarding/pbf/path-monitoring-for-pbf>

upvoted 4 times

  **Thanos84** 4 years, 4 months ago

no discussion

upvoted 2 times

An administrator has a requirement to export decrypted traffic from the Palo Alto Networks NGFW to a third-party, deep-level packet inspection appliance.

Which interface type and license feature are necessary to meet the requirement?

- A. Decryption Mirror interface with the Threat Analysis license
- B. Virtual Wire interface with the Decryption Port Export license
- C. Tap interface with the Decryption Port Mirror license
- D. Decryption Mirror interface with the associated Decryption Port Mirror license

Correct Answer: D

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/decryption-concepts/decryption-mirroring>

  **ChiaPet75** Highly Voted 4 years, 2 months ago

Correct: D

Decryption port mirroring allows you to copy decrypted traffic from a firewall and then send it to a traffic collection tool, such as NetWitness or Solera. Decryption mirroring requires a Decryption Port Mirror license. This license is free of charge and you can activate it through the customer support portal.

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-new-features/decryption-features/decryption_mirroring_support_extension#:~:text=Decryption%20port%20mirroring%20allows%20you,through%20the%20customer%20support%20portal.

upvoted 16 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: D

D is correct

upvoted 2 times

  **Pochex** 1 year, 6 months ago

D is correct - This feature enables creating a copy of decrypted traffic from a firewall and sending it to a traffic collection tool. To enable the feature, you must acquire and install the free license. Please refer to <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/network/network-interfaces/decrypt-mirror-interface>


upvoted 2 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-decryption-port-mirroring>


upvoted 3 times

  **NNgiggs** 2 years, 7 months ago

D is correct, Note the decryption mirror interface only appear as an interface type when you install Decryption port mirror license. see step 4 of the configuration guide in the link below

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/configure-decryption-port-mirroring>

upvoted 3 times

  **benfero** 4 years, 2 months ago

D is right.

upvoted 3 times

When is the content inspection performed in the packet flow process?

- A. after the application has been identified
- B. before session lookup
- C. before the packet forwarding process
- D. after the SSL Proxy re-encrypts the packet

Correct Answer: A

Reference:

<https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081>

  **shamhala1228** Highly Voted 4 years ago

I'm thinking C.
Here's my train of thought, let me know what you think.

B and D are certainly not right. A and C could be both technically true, but which is more accurate? A indicates that "after app has been identified", so we can interpret that in the Flow Diagram as the step in App-ID which says "Pattern based application identification" however, considering the Packet Flow Sequence, after the app is identified, there are still several steps that don't lead directly to Content ID. First it checks for policy matches that will allow it (so it might still get dropped). Then it will check if there are any Security Profiles (ContentID) that will be applicable. QoS and SSL Decryption also might occur at this point. My point is there's a whole bunch of stuff still going on between the "app being identified" and content inspection.

My conclusion is that whenever content inspection is performed it's always before packet forwarding. And it is not always the case that it happens immediately after the app has been identified.

upvoted 19 times

  **trashboat** 3 years, 4 months ago

Content inspection isn't always done (e.g. Application Override), but if it is then it either returns 'detection' and security policy is referenced again or 'no detection' and then traffic is re-encrypted (if SSL decrypted), and THEN the packet is forwarded. So since C isn't always true, I feel like A is the correct answer. I can definitely see how a similar argument can be made for C though, so I agree that both are almost equally correct.

upvoted 3 times

  **ochc** 3 years, 9 months ago

agree. besides, if app is not identified, when it arrives to content inspection it just will not be inspected. so since apps are NOT always identified A cant be. however, both App ID and Content ID ALWAYS happen before packet forwarding process

upvoted 2 times

  **Acidscars** Highly Voted 3 years, 6 months ago

I feel like this question could be simply asked as "When do you learn to read?"

A: After you are done being a toddler

C: Sometime before you die of old age

Technically both are correct. Seriously Palo? Are we supposed to play the choose the more correct answer game? C feels like the broader safer answer. If the Application is Incomplete or Insufficient Data and can't be identified, that doesn't stop Palo from attempting content inspection so it would make A questionable.

upvoted 17 times

  **apiloran** Most Recent 1 month, 3 weeks ago

Selected Answer: A

Content inspection occurred after the session app identified. If app not identified, it would be app override policy match >> pattern based app identification >> security policy lookup based on app >> Rule match with action allowed >> Content inspection

upvoted 1 times

  **hcir** 2 months, 3 weeks ago

C is not possible because there are several options before packet forwarding, content inspection is one of them. content inspection only happens if the traffic has gone through the app-id engine

upvoted 1 times



  **nolox** 3 months, 2 weeks ago

Selected Answer: C

According to this Before the packet forwarding is "closer"

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVHCA0>

upvoted 1 times

  **aurang** 6 months, 1 week ago

A. after the application has been identified

Content inspection is typically performed after the application has been identified in the packet flow process of many firewall systems, including Palo Alto Networks firewalls. This allows for the content of the packets to be inspected for threats and policy violations based on the identified application.


upvoted 1 times

  **franko_72** 7 months, 1 week ago

My two cents. It's C. Scroll down to section 6, Content Inspection, happens right before Forwarding/Egress.



<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVHCA0>

upvoted 1 times

  **ms997** 8 months ago

Answer: A

upvoted 1 times

  **gc999** 9 months, 2 weeks ago

Selected Answer: A

Can find the answer here, which is the same as Question 65.

<https://live.paloaltonetworks.com//t5/image/serverpage/image-id/12862i950F549C7D4E6309>

upvoted 2 times

  **Micutzu** 10 months, 3 weeks ago

Selected Answer: A

The content inspection is performed ONLY if application is identified. If it's an unknown app then the content inspection doesn't happen but the packet it's forwarded, if the security policy allow.

upvoted 3 times

  **Betty2022** 1 year, 1 month ago

Selected Answer: A

Agree A:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVHCA0>

SECTION 5: APPLICATION IDENTIFICATION (APP - ID)

SECTION 6: CONTENT INSPECTION

SECTION 7: FORWARDING/EGRESS

upvoted 4 times

  **Frightened_Acrobat** 1 year, 1 month ago

Selected Answer: C



I'm going to have to go with option C here. A and D both are technically correct. However, A and D are both not necessary steps in the process. C is a necessary step. This is one of those "which is the better answer" scenarios.

upvoted 1 times

  **ChiaPet75** 1 year, 2 months ago

Outside of this flow diagram I couldn't find anything concrete in any docs. Based on the flow diagram you can see there is a question "Session App Identified?", if the answer is "No" then it is sent to the App-ID process before being sent back to the FW Fastpath process. If Content Inspection is applicable then the packet is sent onward to that process.<https://live.paloaltonetworks.com//t5/image/serverpage/image-id/12862i950F549C7D4E6309>

upvoted 1 times

  **Techn** 1 year, 2 months ago

A is correct

"The firewall first performs an application-override policy lookup to see if there is a rule match. If there is, the application is known and content inspection is skipped for this session .

If there is no application-override rule, then application signatures are used to identify the application. The firewall uses protocol decoding in the content inspection stage to determine if an application changes from one application to another ."

upvoted 2 times

  **Betty2022** 1 year, 1 month ago

Agree A:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVHCA0>

SECTION 5: APPLICATION IDENTIFICATION (APP - ID)

SECTION 6: CONTENT INSPECTION

SECTION 7: FORWARDING/EGRESS

upvoted 1 times

  **liericky88** 1 year, 3 months ago

Selected Answer: C

A. could be correct if the wording is "after identifying application" but it's not necessarily have to be successfully identified.

C. is more likely.

upvoted 1 times

  **[Removed]** 1 year, 5 months ago

Selected Answer: C

after app identification there is a return to the previous step before content inspection, recheck the diagram
upvoted 1 times

  **PaloSteve** 1 year, 1 month ago

So this analysis makes both A and C right.

Content inspection happens "after the application has been identified" but "before the packet forwarding process". LOL.

upvoted 1 times

  **Pallab_Kundu** 1 year, 5 months ago

Selected Answer: C

C is correct

upvoted 1 times



An administrator has created an SSL Decryption policy rule that decrypts SSL sessions on any port.
Which log entry can the administrator use to verify that sessions are being decrypted?

- A. In the details of the Traffic log entries
- B. Decryption log
- C. Data Filtering log
- D. In the details of the Threat log entries

Correct Answer: A

Reference:

<https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Implement-and-Test-SSL-Decryption/ta-p/59719>

  **bmarks** Highly Voted 3 years, 6 months ago

PCNSE 9 is current exam content [02/2021] *** ANSWER = A ***

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClboCAC>

The Question is simply asking how to verify if traffic was being decrypted. There are (2) ways to see this in the traffic logs:

1. To confirm that the traffic is decrypted inside the WebGUI > Monitor > Logs > Traffic. Click the magnifying glass icon in the traffic log entries to confirm that the connections were decrypted.
2. Another way to validate the decrypted session is by enabling the column "Decrypted" as below Traffic logs . This can be done by clicking on the arrow down next to any column title and selecting the Columns > Decrypted. This shows decrypted status in regular traffic log view.

upvoted 11 times

  **Barry_Allen** 3 years, 6 months ago



how about PCNSE 10 is it in march of 2021 or still PCNSE 9 in march... ?

upvoted 1 times

  **lucaboban** 3 years, 5 months ago

As of, August 17th 2020, the Palo Alto Networks Certified Network Security Engineer (PCNSE) and the Palo Alto Networks Certified Network Security Administrator (PCNSA) certification exams reflect changes based on PAN-OS 10.0.

upvoted 1 times

  **Biz90** 2 years, 10 months ago

Excellent answer :)

upvoted 1 times

  **scanossa** 9 months, 4 weeks ago

And on the Traffic logs, you can also add the "Decrypted" column, which would show Yes or No in case the connection was decrypted or not

upvoted 2 times

  **PA** Highly Voted 4 years, 10 months ago

I think its A.

upvoted 7 times

  **kambata** Most Recent 2 months ago

Selected Answer: A

By default decryption logs only unsuccessful events A is correct.

upvoted 1 times

  **8f3e6ca** 3 months, 2 weeks ago

Another stupid question with 2 answers. Both A and B are correct.

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/verify-decryption>

After you configure a best practice decryption profile and apply it to traffic, you can check both the Decryption logs (introduced in PAN-OS 10.0) and the Traffic logs to verify that the firewall is decrypting the traffic.

upvoted 1 times

  **jens23** 6 months ago

Selected Answer: A



By default, Decryption policies only log unsuccessful TLS handshakes.

upvoted 2 times

  **kambata** 2 months ago

True !

upvoted 1 times

  **JRKhan** 7 months, 4 weeks ago

Selected Answer: A

I would lean towards option A as the question asks about how one can go about verifying if sessions are being decrypted. In the details of traffic log entry, you can check if the decrypt flag is marked or not. The decrypted log file introduced in PAN OS 10 on the other hand provides comprehensive information about individual session that are decrypted, the sessions that are marked for "no decrypt" in the decryption policy or any global protect sessions when you enable decryption logging in the global protect portal or gateway configuration.



upvoted 2 times

  **dorf05** 9 months ago

Selected Answer: B

[https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/troubleshoot-and-monitor-decryption/decryption-logs#:~:text=The%20Decryption%20Log%20\(MonitorLogsDecryption\)%20provides%20comprehensive%20information%20about%20sessions%20that%20match%20a%20Decryption%20policy%20to%20help%20you%20gain%20context%20about%20that%20traffic%20so%20you%20can%20accurately%20and%20easily%20diagnose%20and%20resolve%20decryption%20issues](https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/troubleshoot-and-monitor-decryption/decryption-logs#:~:text=The%20Decryption%20Log%20(MonitorLogsDecryption)%20provides%20comprehensive%20information%20about%20sessions%20that%20match%20a%20Decryption%20policy%20to%20help%20you%20gain%20context%20about%20that%20traffic%20so%20you%20can%20accurately%20and%20easily%20diagnose%20and%20resolve%20decryption%20issues)

upvoted 1 times

  **ms997** 9 months, 1 week ago

Answer:A is say clear when to find Decrypted. in traffic logs

upvoted 1 times

  **techplus** 9 months, 2 weeks ago

Selected Answer: B

Decryption Log

upvoted 1 times


  **Xuzi** 10 months ago

Very clear answer on PA website

After you configure a best practice decryption profile and apply it to traffic, you can check both the Decryption logs

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/verify-decryption>

upvoted 1 times

  **Micutzu** 10 months, 3 weeks ago

Selected Answer: A

The question t's about log ENTRY and not log TYPE.

upvoted 1 times

  **techplus** 11 months ago

Selected Answer: B

Decryption log is where you see what its being decrypted, the system log is to see if there is any issues with the decryption policy

upvoted 1 times

  **Betty2022** 1 year, 1 month ago

Selected Answer: A

as per bmarks and links shared. Agree

upvoted 1 times

  **Frightened_Acrobat** 1 year, 1 month ago

Selected Answer: A

Again, best answer. As Pochex pointed out Decryption logs don't show all traffic, so using traffic logs and looking at the decryption field is your best option to 'verify' decryption is occuring or not.

upvoted 1 times

  **kewokil120** 1 year, 4 months ago

Selected Answer: A

The answer is a. In traffic details you will see proxy/decryption checkbox

upvoted 1 times

  **BryanSalazar** 1 year, 5 months ago

Selected Answer: A

Its A, just tested in my lab

upvoted 1 times

  **aaccnp** 1 year, 5 months ago

Selected Answer: B

B

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/troubleshoot-and-monitor-decryption#ida09e44a8-fd80-41e8-8572-33e9b122ad22>

upvoted 2 times

An administrator has been asked to configure a Palo Alto Networks NGFW to provide protection against external hosts attempting to exploit a flaw in an operating system on an internal system.

Which Security Profile type will prevent this attack?

- A. Vulnerability Protection
- B. Anti-Spyware
- C. URL Filtering
- D. Antivirus


Correct Answer: A

Reference:


<https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/objects/objects-security-profiles-vulnerability-protection>

  **guilherme_a** Highly Voted 4 years ago

A is correct. Because anti-spyware has identified compromised outgoing traffic. Vulnerability Protection identifies incoming traffic.
upvoted 9 times


  **benfero** Highly Voted 4 years, 2 months ago

A is correct
upvoted 5 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: A

A is correct
upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago



Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/objects/objects-security-profiles-vulnerability-protection>
upvoted 2 times



  **UFanat** 2 years, 2 months ago

Selected Answer: A

A is correct
upvoted 2 times

  **Biz90** 2 years, 10 months ago

Answer here is A. Key word here is 'Flaw' that a flaw can be classed as a vulnerability, in which can then be further exploited by an attacker.
upvoted 3 times

  **lol1000** 3 years, 10 months ago

a

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-web-interface-help/objects/objects-security-profiles-vulnerability-protection.html>
upvoted 4 times

Which processing order will be enabled when a Panorama administrator selects the setting `Objects defined in ancestors will take higher precedence?`

- A. Descendant objects will take precedence over other descendant objects.
- B. Descendant objects will take precedence over ancestor objects.
- C. Ancestor objects will have precedence over descendant objects.
- D. Ancestor objects will have precedence over other ancestor objects.

Correct Answer: C

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-setup-management>

  **rammsdoct** Highly Voted 4 years, 2 months ago

Yep Correct C :
upvoted 9 times



  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: C

C is correct
upvoted 1 times

  **scanossa** 8 months ago

I got this question in the exam
upvoted 3 times

  **DenskyDen** 1 year, 7 months ago

Selected Answer: C

By default, when device groups at different levels in the Device Group Hierarchy have an object with the same name but different values (because of overrides, as an example), policy rules in a descendant device group use the object values in that descendant instead of using object values inherited from ancestor device groups. Optionally, you can reverse this order of precedence to push values from the highest ancestor containing the object to all descendant device groups. After you enable this option, the next time you push configuration changes to device groups, the values of inherited objects replace the values of any overridden objects in the descendant device groups.



upvoted 3 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/manage-device-groups/manage-precedence-of-inherited-objects>

upvoted 4 times

  **Gabuu** 2 years, 7 months ago

C is true
upvoted 3 times

  **Kane002** 2 years, 9 months ago

Even a person totally ignorant of PA could only come to the conclusion of C or D, just based off the wording of the question. But it's C, descendants are taken to be more particular, and are by default overriding ancestor settings.



upvoted 3 times

  **Sammy3637** 4 years, 8 months ago

<https://docs.paloaltonetworks.com/panorama/7-1/panorama-admin/manage-firewalls/manage-precedence-of-inherited-objects>
upvoted 3 times

  **zadkiel** 4 years, 1 month ago

so, B right?
upvoted 1 times

  **zadkiel** 4 years, 1 month ago

sorry, C is correct
upvoted 2 times

An administrator using an enterprise PKI needs to establish a unique chain of trust to ensure mutual authentication between Panorama and the managed firewalls and Log Collectors.

How would the administrator establish the chain of trust?

- A. Use custom certificates
- B. Enable LDAP or RADIUS integration
- C. Set up multi-factor authentication
- D. Configure strong password authentication

Correct Answer: A

Reference:

https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/panorama-overview/plan-your-panorama-deployment

  **rammsdoct** Highly Voted 4 years, 2 months ago

Yes A:

clarifying:

<https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/set-up-panorama/set-up-authentication-using-custom-certificates>
upvoted 8 times

  **lol1000** Highly Voted 3 years, 10 months ago

a

<https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/set-up-panorama/set-up-authentication-using-custom-certificates.html>
upvoted 6 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: A

A is correcc

upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/set-up-panorama/set-up-authentication-using-custom-certificates>
upvoted 2 times

  **Prutser2** 3 years, 2 months ago

says PKI all but A have anythng to do with that

upvoted 3 times

What will be the egress interface if the traffic's ingress interface is ethernet1/6 sourcing from 192.168.111.3 and to the destination 10.46.41.113 during the time shown in the image?

```
admin@Lab33-111-PA-3060(active)> show clock
```

```
Thu Jun 8 12:49:55 PDT 2017
```

```
#####
```

```
admin@Lab33-111-PA-3060(active)# show vsys vsys1 rulebase pbf rules test-pbf
```

```
test-pbf {
  action {
    forward {
      egress-interface ethernet1/5;
    }
  }
  from {
    zone L3-Trust;
  }
  enforce-symmetric-return {
    enabled no;
  }
  source 192.168.111.3;
  destination 10.46.41.113;
  source-user any;
  application any;
  service any;
  schedule schedule-pbf;
}
```

```
#####
```

```
admin@Lab33-111-PA-3060(active)# show vsys vsys1 schedule schedule-pbf
```

```
schedule-pbf {
  schedule-type {
    recurring {
      daily 16:00-21:00;
    }
  }
}
```



```
#####
```

```
admin@Lab33-111-PA-3060(active)> show routing fib
```

id	destination	nexthop	flags	interface	mtu
47	0.0.0.0/0	10.46.40.1	ug	ethernet1/3	1500
67	10.10.20.0/24	0.0.0.0	u	ethernet1/7	1500
66	10.10.20.111/32	0.0.0.0	uh	ethernet1/7	1500
46	10.46.40.0/23	0.0.0.0	u	ethernet1/3	1500
49	10.46.44.0/23	0.0.0.0	u	ethernet1/5	1500
45	10.46.41.111/32	0.0.0.0	uh	ethernet1/3	1500
70	10.46.41.113/32	10.46.40.1	ug	ethernet1/3	1500
48	10.46.45.111/32	0.0.0.0	uh	ethernet1/5	1500
51	192.168.111.0/24	0.0.0.0	u	ethernet1/6	1500
50	192.168.111.2/32	0.0.0.0	uh	ethernet1/6	1500

- A. ethernet1/7
- B. ethernet1/5
- C. ethernet1/6
- D. ethernet1/3

Correct Answer: D

  **shetoshandasa** Highly Voted 3 years, 5 months ago

The answer is D, because current time is outside the scheduled time
upvoted 10 times


  **Qintao** Highly Voted 3 years, 4 months ago

D.
PBF is to e1/5, but the current time is not in time schedule. the normal routing will go to e1/3
upvoted 6 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: D

Answer is D
upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

D. PBF + schedule is not on par with the current time the traffic was generated.
upvoted 1 times

  **secdaddy** 2 years, 1 month ago

English error in the question adds confusion. Should be "...at the time shown" and not "...during the time shown" as during = range and the only range shown is that in the scheduler.

upvoted 1 times

  **Chandera** 2 years, 6 months ago

Answer is D

Because in routing longest prefix match is preferred and for 10.46.41.113/32 egress interface is eth1/3

upvoted 2 times

  **confusion** 2 years, 6 months ago

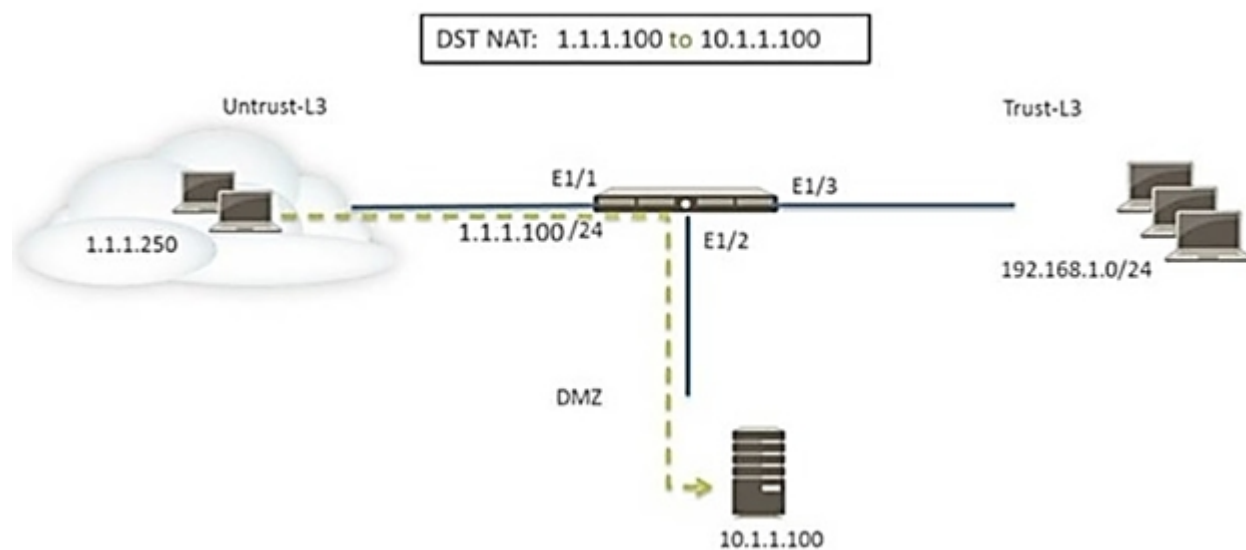
Selected Answer: D

D.

PBF + schedule for it, but current time is not within the schedule, so normal routing occurs.

upvoted 4 times

Refer to the exhibit. A web server in the DMZ is being mapped to a public address through DNAT.



Which Security policy rule will allow traffic to flow to the web server?

- A. Untrust (any) to Untrust (10.1.1.100), web browsing ɾ Allow
- B. Untrust (any) to Untrust (1.1.1.100), web browsing ɾ Allow
- C. Untrust (any) to DMZ (1.1.1.100), web browsing ɾ Allow
- D. Untrust (any) to DMZ (10.1.1.100), web browsing ɾ Allow

Correct Answer: C

trashboat Highly Voted 3 years, 4 months ago

C is the correct answer.

Remember for Security Policy lookup, the firewall uses Pre-NAT IP and Post-NAT Zone.

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/networking/nat/nat-policy-rules/nat-policy-overview.html>
upvoted 13 times

Yuval711 Most Recent 2 months, 2 weeks ago

Selected Answer: D

D is the correct answer.

the question is about security policy and the destination is 10.1.1.100

upvoted 1 times

Marshpillowz 7 months, 2 weeks ago

Selected Answer: C

Answer is C

upvoted 1 times

mbhuyan 1 year, 3 months ago

Selected Answer: B

Answer should B

upvoted 2 times

Woody 1 year, 8 months ago

Should that not be D based on <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/nat/nat-configuration-examples/destination-nat-with-port-translation-example#id053beeb9-fde0-445b-99d0-5dd5a1000b7c> ?

upvoted 1 times

DenskyDen 1 year, 7 months ago

that should be C as mentioned on the question, it was natted.

upvoted 1 times

TAKUM1y 1 year, 11 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/nat/nat-policy-rules/nat-policy-overview>

upvoted 2 times

confusion 2 years, 6 months ago

Selected Answer: C

C. because security policy is pre-NAT IP + post-NAT ZONE.

upvoted 4 times

  **Kane002** 2 years, 9 months ago

C is correct. I got this question on the PCNSA, and so I wouldn't expect to see it on the PCNSE.

upvoted 3 times

  **Angel123** 3 years, 3 months ago

I believe the correct answer is 'B'

Since this is DNAT setup, rule for security policy is: PRE-NAT addresses, POST-NAT zone.

PCNSA study guide PAN OS 10.0, p.111

upvoted 2 times

  **Angel123** 3 years, 3 months ago

Pardon me - 'C' is the answer with POST-NAT zone.



upvoted 4 times

  **shetoshandasa** 3 years, 5 months ago

Correct Answer

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destination-nat-exampleone-to-many-mapping>

upvoted 1 times

  **mmed** 3 years, 5 months ago

the corrct answer is D

upvoted 1 times

  **webmanau** 3 years, 5 months ago

No it's not. C is correct. the pre-NAT address is required as the destination in the security rule

upvoted 3 times

  **Prutser2** 3 years, 2 months ago

no, C, It then evaluates and applies any security policies that match the packet based on the original (pre-NAT) source and destination addresses, but the post-NAT zones

upvoted 1 times

A web server is hosted in the DMZ and the server is configured to listen for incoming connections on TCP port 443. A Security policies rules allowing access from the Trust zone to the DMZ zone needs to be configured to allow web-browsing access. The web server hosts its contents over HTTP(S). Traffic from Trust to DMZ is being decrypted with a Forward Proxy rule.

Which combination of service and application, and order of Security policy rules, needs to be configured to allow cleartext web-browsing traffic to this server on tcp/443?

- A. Rule #1: application: web-browsing; service: application-default; action: allow Rule #2: application: ssl; service: application-default; action: allow
- B. Rule #1: application: web-browsing; service: service-http; action: allow Rule #2: application: ssl; service: application-default; action: allow
- C. Rule # 1: application: ssl; service: application-default; action: allow Rule #2: application: web-browsing; service: application-default; action: allow
- D. Rule #1: application: web-browsing; service: service-https; action: allow Rule #2: application: ssl; service: application-default; action: allow

Correct Answer: D

YasserSaied Highly Voted 3 years, 2 months ago

D -- Server hosts HTTP/HTTPS both on Port 443 .. that means to access the HTTP on port 443, web-browsing "Application" need to be enabled on "service-https" service

upvoted 11 times

Prutser2 3 years, 2 months ago

in addition, rule 2 is to allow the incoming encrypted SSL traffic, and once decrypted, rule1 will allow web browsing on port 443, cos that is what the server is listening on, so D

upvoted 3 times

trashboat Highly Voted 3 years, 4 months ago

A is the correct answer. The TCP session will be built and hit the SSL decryption policy, which will decrypt the packets and forward them on HTTP via TCP/443 - this is behavior for PAN-OS 10.0+.

That being said, I also think the first rule in A would suffice to allow the traffic.

upvoted 8 times

confusion 2 years, 5 months ago

A and C are exactly the same, there must be something wrong in these answers.

upvoted 1 times

confusion 1 year, 10 months ago

ignore that!

upvoted 1 times

Elvenking 2 years, 4 months ago

A is wrong.

The first rule uses application-default, so no match there when "web-browsing" is changed to while app inspection is remade after decryption. It needs be service at port 443 explicitly.

upvoted 1 times

datz 2 years, 3 months ago

A is wrong app-default on web browsing - wont allow 443

upvoted 1 times

Eluis007 Most Recent 5 months ago

A rule would allow the web traffic to pass over both, 80 and 443,

D rule would allow just over 443, so D

upvoted 1 times

Jared28 6 months ago

Selected Answer: C

As was mentioned below, for a bit now the app-id web-browsing shows a default secure port of TCP 443. So *when ssl is decrypted* and the decrypted traffic matches web-browsing, TCP 443 will be allowed with app-default.

upvoted 2 times

DatITGuyTho1337 8 months, 2 weeks ago

Voting for answer A, due to this article "<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/application-default>"

upvoted 2 times

[-] **Micutzu** 10 months, 3 weeks ago

Selected Answer: D

I think that all the options are valid to allow cleartext web-browsing traffic on tcp/443. The most precise rule is D.
upvoted 1 times

[-] **Eiffelsturm** 1 year, 2 months ago

So D was correct before the default secure ports were introduced I think. You can see them in the GUI. According to this KB article <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIHqCAK> with Decryption enabled those applications are identified correctly as e.g. web-browsing if it's active on 443 and the Security Policy with "application-default" will allow it. The question is if the Exam is this up to date :D
upvoted 1 times

[-] **hz78** 1 year, 4 months ago

B is correct. In option D, the first Security policy rule allows web-browsing traffic on the HTTPS service (service-https), which is not applicable in this scenario since the web server is configured to host its contents over HTTP(S) and is listening on TCP port 443 for incoming connections.

If we allow the web-browsing application traffic using the HTTPS service, the firewall will forward the traffic to the web server without decrypting it, since it is HTTPS traffic. However, the web server is hosting its contents over HTTP(S), so the firewall needs to decrypt the traffic before forwarding it to the web server.

Therefore, the correct service to be used in the first Security policy rule is service-http instead of service-https. This will allow the firewall to decrypt the traffic before forwarding it to the web server and also allow web-browsing traffic from the Trust zone to the DMZ zone.

Hence, option B is the correct answer.

upvoted 2 times

[-] **Frightened_Acrobat** 1 year, 6 months ago

I agree D. However, the way the question is worded and answers are very tricky. It's not the way you'd go about explaining this or executing the solution IRL. Shame on Palo Alto for trying to mislead us purposely on questions like this. I mean we only have an average of 1 min, 4sec per question.

Rule 2 is unnecessary to allow cleartext, which is the stated goal of the question. No decryption is necessary for the firewall to identify cleartext web-browsing traffic. A bad question overall.

upvoted 4 times

[-] **Bruno_Nascimento** 1 year, 7 months ago

The correct Answer is A.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/application-default>

upvoted 3 times

[-] **DatITGuyTho1337** 8 months, 2 weeks ago

I agree, especially after reading the article!

upvoted 1 times

[-] **Chris71Mach1** 1 year, 7 months ago

Selected Answer: D

I didn't even get to rule 2 before I knew D was the right answer. It's the only one that lists the application as web-browsing and the service as HTTPS.

upvoted 2 times

[-] **spydog** 1 year, 11 months ago

Selected Answer: A

Starting from PanOS 9.0 answer A is correct.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/application-default>

Couple of applications are defined with "standard" and "secure" ports, which allow you to use application web-browsing with application-default ports, after decryption.

First rule from A will match the traffic after decryption. Second rule is needed to allow the initial connection to be established. Traffic will be initially allowed over second rule and after decryption application will shift and new lookup will match first rule

upvoted 3 times

[-] **juan_L** 2 years ago

C -- Is the correct, On first packets application will be identified as SSL, once the tunnel established (after TLS hello exchanging between Client and Server, cipher chosen.... dears check TLS negotiation wikis) the firewall starts to decrypt via proxy forward, in that moment the app is identified as web-browsing. The TLS tunnel must be negotiated first and this handshake will be identified as SSL.

upvoted 2 times

[-] **Pretorian** 2 years, 1 month ago

If you go to objects > applications (applipedia doesn't show this) and search for "web-browsing" open that signature and locate the field "standard port" and "secure port" you'll see port 80 and 443.

This means that if you create a policy allowing web-browsing with application default, this app will be allowed on both of those ports.

Now you no longer need to create a policy allowing SSL on port 443 before your policy allowing web-browsing. This is now from the past. This is true for a handful of applications only at this point.

Which means that this question might show an answer along those lines if it ever gets updated.

upvoted 4 times

  **Pretorian** 2 years, 1 month ago

If you go to objects > applications (appipedia doesn't show this) and search for "web-browsing" open that signature and locate the field "standard port" and "secure port" you'll see port 80 and 443.

This means that if you create a policy allowing web-browsing with application default, this app will be allowed on both of those ports.

Now you no longer need to create a policy allowing SSL on port 443 before your policy allowing web-browsing. This is now from the past. This is true for a handful of applications only at this point.

Which means that this question might show an answer Long those lines if it ever gets updated.

upvoted 1 times

  **secdaddy** 2 years, 1 month ago


goal : cleartext (web-browsing/http) on tcp/443

server hosts both http and https on 443

web-browsing on 443 must be checked before SSL application on 443 drops the packet

http application-default = 80 so must use service-https for 443 (only D)

upvoted 1 times

  **DatITGuyTho1337** 8 months, 2 weeks ago

application default ports for web-browsing app is 80 and 443, so it means the firewall will consider both when processing. I don't think you need a separate rule for to answer the question.

upvoted 1 times

  **Skirka** 2 years, 1 month ago

Selected Answer: D

Should be

upvoted 1 times

Which two options prevent the firewall from capturing traffic passing through it? (Choose two.)

- A. The firewall is in multi-vsyst mode.
- B. The traffic is offloaded.
- C. The traffic does not match the packet capture filter.
- D. The firewall's DP CPU is higher than 50%.

Correct Answer: BC

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/take-packet-captures/disable-hardware-offload>


  **zhawk7661** Highly Voted 4 years, 1 month ago

ANSWER: B, C
upvoted 9 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: BC

B and C are correct
upvoted 1 times


  **Techn** 1 year, 2 months ago

Answer is B&C
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CldYCAS>
upvoted 1 times

  **Knowledge33** 1 year, 3 months ago

Selected Answer: BC

it's ba and c
upvoted 1 times

  **hpbdc** 1 year, 11 months ago

Selected Answer: BC

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/take-packet-captures/disable-hardware-offload>
upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: BC

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/take-packet-captures/disable-hardware-offload#id6ee2fc62-e4c3-42cb-9b1e-72cf11ebdd66>
upvoted 2 times

  **JMIB** 2 years ago

Correct Answer: BC (Only - The Traffic)
B. The Traffic
C. The Traffic
upvoted 1 times

  **s4murai** 3 years, 6 months ago

Answer should be B and C
upvoted 3 times

A global corporate office has a large-scale network with only one User-ID agent, which creates a bottleneck near the User-ID agent server. Which solution in PAN-OS® software would help in this case?

- A. application override
- B. Virtual Wire mode
- C. content inspection
- D. redistribution of user mappings

Correct Answer: D

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/user-id/deploy-user-id-in-a-large-scale-network>



  **purushothaman** Highly Voted 4 years, 2 months ago

Answer is D
upvoted 10 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: D

Answer is D
upvoted 1 times

  **GohanF2** 1 year, 6 months ago

This question appeared on the exam on January. 2023.
upvoted 3 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/deploy-user-id-in-a-large-scale-network>
upvoted 3 times

  **DriVen** 2 years, 1 month ago

Override is for APP ID, Virtual Wire is for network, Inspection is for content, only logical answer here is D!
upvoted 4 times

An administrator has been asked to create 100 virtual firewalls in a local, on-premise lab environment (not in the cloud). Bootstrapping is the most expedient way to perform this task.

Which option describes deployment of a bootstrap package in an on-premise virtual environment?

- A. Use config-drive on a USB stick.
- B. Use an S3 bucket with an ISO.
- C. Create and attach a virtual hard disk (VHD).
- D. Use a virtual CD-ROM with an ISO.

Correct Answer: D

Reference:

<https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization/set-up-the-vm-series-firewall-on-kvm/install-the-vm-series-firewall-on-kvm/use-an-iso-file-to-deploy-the-vm-series-firewall>

  **ChiaPet75** Highly Voted 4 years, 2 months ago

Correct: D

<https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/bootstrap-the-vm-series-firewall/bootstrap-package>
upvoted 7 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago



Selected Answer: D

Correct answer is D
upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/vm-series/10-2/vm-series-deployment/set-up-the-vm-series-firewall-on-kvm/install-the-vm-series-firewall-on-kvm>
upvoted 3 times

  **lol1000** 3 years, 10 months ago

d
<https://docs.paloaltonetworks.com/vm-series/10-0/vm-series-deployment/bootstrap-the-vm-series-firewall/bootstrap-package.html>
upvoted 4 times

Which two benefits come from assigning a Decryption Profile to a Decryption policy rule with a `No Decrypt` action? (Choose two.)

- A. Block sessions with expired certificates
- B. Block sessions with client authentication
- C. Block sessions with unsupported cipher suites
- D. Block sessions with untrusted issuers
- E. Block credential phishing

Correct Answer: AD

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/define-traffic-to-decrypt/create-a-decryption-profile>

  **djedeem** Highly Voted 1 year, 7 months ago

A,C,D are all correct for this question:

Depending on your needs, create Decryption profiles to:

Block sessions based on certificate status, including blocking sessions with >>>expired certificates, >>>untrusted issuers, unknown certificate status, certificate status check timeouts, and certificate extensions.

Block sessions with >>>unsupported versions and cipher suites, and that require using client authentication.

upvoted 5 times

  **kambata** Most Recent 2 months ago

Selected Answer: AC

A and C, checked on an actual firewall, those are the only settings in NO DECRYPT.

upvoted 2 times

  **Pnosuke** 7 months, 1 week ago

Here is the documentation for A and D.

<https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/decryption/decryption-concepts/no-decryption-decryption-profile#id185BA08H0PP>

upvoted 1 times

  **Pnosuke** 7 months, 1 week ago

A and D are correct.

"No Decryption" is the Keyword of this question.

There are following 2 items in the Server Certificate Verification in the No Decryption configuration.

- Block sessions with expired certificates
- Block sessions with untrusted issuers



upvoted 1 times

  **Marshpillowz** 7 months, 2 weeks ago

Selected Answer: AD

A and D correct

upvoted 1 times

  **Nawda** 11 months, 3 weeks ago

Selected Answer: CD



V as well

upvoted 1 times

  **Nawda** 11 months, 3 weeks ago

I meant c

upvoted 1 times

  **lildevil** 1 year, 2 months ago

A C & D are correct based on <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/define-traffic-to-decrypt/create-a-decryption-profile>

upvoted 2 times

  **studycerts** 1 year, 9 months ago



Selected Answer: AD

Not sure about this question, as the URL below says this:



Block sessions based on certificate status, including blocking sessions with expired certificates, untrusted issuers, unknown certificate status, certificate status check timeouts, and certificate extensions.

Block sessions with unsupported versions and cipher suites, and that require using client authentication.
So theoretically A, C, and D seem to be correct, but we only need to chose 2?

upvoted 3 times

  **dians** 1 year, 9 months ago


C is not correct because of the action "No decrypt", it's not relevant to talk about cipher suites in this case because there is no decryption
upvoted 4 times

  **obatel** 1 year, 9 months ago



The "No decrypt" in the question does not make C incorrect. Unsupported cipher is also a benefit of the decryption profile. There is a BitTorrent question earlier that a decryption profile due to unsupported cipher was given as the answer.
upvoted 3 times

  **markeloff23** 1 year, 5 months ago

yes, see bittorrent question
upvoted 1 times

  **Techn** 1 year, 2 months ago

exactly,
<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-concepts/no-decryption-decryption-profile>
upvoted 2 times

  **fireb** 1 year, 10 months ago

A & D are the correct options.
upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: AD

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/define-traffic-to-decrypt/create-a-decryption-profile>
upvoted 2 times



Which User-ID method should be configured to map IP addresses to usernames for users connected through a terminal server?

- A. port mapping
- B. server monitoring
- C. client probing
- D. XFF headers

Correct Answer: A

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/configure-user-mapping-for-terminal-server-users>

  **sethjam** Highly Voted 4 years, 2 months ago

Ans. A

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-mapping-for-terminal-server-users>

upvoted 8 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: A

A is correct


upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: A



<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-mapping-for-terminal-server-users>

upvoted 1 times

  **Gabuu** 2 years, 1 month ago

A is the answer

upvoted 1 times

  **lol1000** 3 years, 10 months ago

a

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-mapping-for-terminal-server-users.html>

upvoted 4 times

Which feature can be configured on VM-Series firewalls?

- A. aggregate interfaces
- B. machine learning
- C. multiple virtual systems
- D. GlobalProtect

Correct Answer: D

  **zhawk7661** Highly Voted 4 years, 1 month ago

ANSWER: D

upvoted 7 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: D

Answer is D - Global Protect

upvoted 1 times

  **secdaddy** 2 years, 1 month ago

All Palo Alto Networks firewalls except the VM-Series models support AE interface groups.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/network/network-interfaces/aggregate-ethernet-ae-interface-group>

upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: D

GlobalProtect can be configured

upvoted 2 times

  **eyelasers1** 2 years, 6 months ago

Not Virtual systems C: <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/virtual-systems/virtual-systems-overview/platform-support-and-licensing-for-virtual-systems.html>

upvoted 1 times

  **gordonF** 3 years, 7 months ago

D for sure, but can not ignore A as well.

upvoted 2 times

  **nirzuk** 4 years ago

this now should in cloud Option B - Machine Learning also, since PAN-OS 10 supports ML

upvoted 3 times

  **anak1n** 3 years, 5 months ago

is a difference between "this could", "this should" ;)

upvoted 1 times

In High Availability, which information is transferred via the HA data link?

- A. session information
- B. heartbeats
- C. HA state information
- D. User-ID information

Correct Answer: A

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/high-availability/ha-concepts/ha-links-and-backup-links>

  **lol1000** Highly Voted 3 years, 10 months ago

a

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/high-availability/ha-concepts/ha-links-and-backup-links.html>

upvoted 6 times

  **cthd** Highly Voted 4 years, 2 months ago

ha data link = HA2 = sync session

upvoted 5 times

  **Marshpillowz** Most Recent 7 months, 2 weeks ago

Selected Answer: A

Correct answer is A

upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/ha-links-and-backup-links>



upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: A

A. HA data link is designed mainly for exchanging session information

upvoted 2 times

  **FS68** 2 years, 11 months ago

A is correct

upvoted 2 times

  **Sammy3637** 4 years, 8 months ago

<https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/high-availability/ha-concepts/ha-links-and-backup-links>

upvoted 3 times

The firewall identifies a popular application as an unknown-tcp.

Which two options are available to identify the application? (Choose two.)

- A. Create a custom application.
- B. Create a custom object for the custom application server to identify the custom application.
- C. Submit an App-ID request to Palo Alto Networks.
- D. Create a Security policy to identify the custom application.

Correct Answer: AC

  **Edu147** Highly Voted 5 years, 1 month ago

Correct A, C

C is not apple-id, is app-id

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/app-id/manage-custom-or-unknown-applications#>

upvoted 17 times

  **ochc** Highly Voted 3 years, 9 months ago

The statement says "The firewall identifies a popular application as an unknown-tcp". It doesn't say traffic is being dropped. If it identifies it, that means a rule is already in place. It also says popular, and as per <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/manage-custom-or-unknown-applications#>, "...If the packet capture reveals that the application is a commercial application, you can submit this packet capture to Palo Alto Networks for App-ID development...". Commercial equates to popular. I say AC



upvoted 9 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: AC

A and C correct.

upvoted 1 times

  **Techn** 1 year, 2 months ago

A&C is correct:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clu2CAC>

upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: AC

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/manage-custom-or-unknown-applications>

upvoted 3 times

  **Kuronekosama** 2 years ago

Selected Answer: AD

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/manage-custom-or-unknown-applications>

Actually shows A,C,D as all viable options. Great...

I think A & D actually provide solutions, versus waiting on Palo to build you something that you will need to wait for.

upvoted 1 times

  **Gabriel2022** 2 years ago

ITs handle not identify ... A&C

Create security policies to control unknown applications by unknown TCP, unknown UDP or by a combination of source zone, destination zone, and IP addresses.

upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: AC

You can create a custom app:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/use-application-objects-in-policy/create-a-custom-application>

or submit a request to PAN

<https://www.paloaltonetworks.com/blog/submit-an-application/>



upvoted 2 times

  **Meira088** 2 years, 3 months ago

Selected Answer: AC

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/app-id/manage-custom-or-unknown-applications#>



upvoted 1 times

  **AbuHussain** 2 years, 5 months ago

Selected Answer: AC

Correct A, C

upvoted 1 times

  **WATU** 2 years, 5 months ago

Correct A, C.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/manage-custom-or-unknown-applications>

Check that the article mentioned "Create security policies to control unknown application" No to Identify as the option D

upvoted 1 times

  **FS68** 2 years, 11 months ago

A C correct

upvoted 2 times

  **anak1n** 3 years, 4 months ago


Go on the Reference link read the beginning and after the step 6, you need to create a custom app and then to create a security policy to allow the new app that you created... during time you will understand how it communicates, how access is done as is written in the tech docs... after that if you want you can submit this to Palo to create an app but 1st you need to do this so the answer is A and D .

upvoted 2 times

  **Elvenking** 2 years, 4 months ago

The question asks for "options" rather than "steps". I guess the question is one of those general knowledge q's.

upvoted 1 times

  **Narendragpt** 3 years, 5 months ago

A and C are correct

upvoted 1 times

  **tuktuk2020** 3 years, 5 months ago

A , C

C: since it is a popular (referred in the docs as "commercial") Application ,

((Request an App-ID from Palo Alto Networks—If you would like to inspect and control the applications that traverse your network, for any unknown traffic, you can record a packet capture. If the packet capture reveals that the application is a commercial application, you can submit this packet capture to Palo Alto Networks for App-ID development. If it is an internal application, you can create a custom App-ID and/or define an application override policy.))

D: would be right if it an internal or Organization Application

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/manage-custom-or-unknown-applications>

upvoted 2 times

  **RinoAlenz** 3 years, 6 months ago

Correct A, D

C "Create a custom application." unconditional.

upvoted 1 times

  **hpbdcb** 3 years, 9 months ago

A & D

A: because thats the way to go to reliably identify a custom app

PA says: "Create a Custom Application with a signature and attach it to a security policy"

D: because you need to see traffic on the wire to create custom patterns matching that new application (otherwise it would be just blocked and you will not be able to create a custom app)

PA says: "Create security policies to control unknown applications by unknown TCP, unknown UDP or by a combination of source zone, destination zone, and IP addresses.

"

So even though a security policy alone (D) will not help but together with A its the way how it works.

ref:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/manage-custom-or-unknown-applications#>

upvoted 1 times

  **Pradeepan** 3 years, 11 months ago

A and c are the answer we can create custom as well give request for app-id creation

upvoted 1 times

If an administrator wants to decrypt SMTP traffic and possesses the server's certificate, which SSL decryption mode will allow the Palo Alto Networks NGFW to inspect traffic to the server?

- A. TLS Bidirectional Inspection
- B. SSL Inbound Inspection
- C. SSH Forward Proxy
- D. SMTP Inbound Decryption

Correct Answer: B

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssl-inbound-inspection>

  **Biz90** Highly Voted 2 years, 10 months ago

The answer is B, there are three types of decryption (excluding a no-decrypt' rule) that one can use on the PA:

1. SSL Forward Proxy - Inside to Outside (To the the internet)
 2. SSL Inbound Proxy - Outside to Inside (usually towards a hosted webserver in your net)
 3. SSH Forward Proxy - As is states, for SSH traffic. The important one to remember for this type of decryption is that no certs are required.
- upvoted 12 times



  **zadkiel** Highly Voted 4 years, 1 month ago

B is correct i think
upvoted 8 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: B

Correct answer is B
upvoted 1 times

  **Techn** 1 year, 2 months ago

question say that '...possesses the server's certificate..' due to B is correct
upvoted 1 times

  **Knowledge33** 1 year, 3 months ago

Selected Answer: B

answer is B
upvoted 1 times

  **Acidscars** 1 year, 5 months ago

I guess B, but its a BS question. Possessing the certificate is only half of what you need. You need the private key as well which is left out from the question.
upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-inbound-inspection>
upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: B

B is a correct one.
A and D do not exist as an option.
C. is not correct because SMTPs uses SSL not SSH
upvoted 2 times

  **guilherme_a** 4 years ago

B is correct
upvoted 4 times

A client has a sensitive application server in their data center and is particularly concerned about resource exhaustion because of distributed denial-of-service attacks.

How can the Palo Alto Networks NGFW be configured to specifically protect this server against resource exhaustion originating from multiple IP addresses (DDoS attack)?

- A. Define a custom App-ID to ensure that only legitimate application traffic reaches the server.
- B. Add a Vulnerability Protection Profile to block the attack.
- C. Add QoS Profiles to throttle incoming requests.
- D. Add a DoS Protection Profile with defined session count.

Correct Answer: D

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules/dos-protection-profiles>

  **zhawk7661** Highly Voted 4 years, 1 month ago

ANSWER: D

upvoted 9 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: D

Correct answer is D

upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules/dos-protection-profiles#ida42d52fa-3366-4695-bb4a-d39ebf3b6a5f>



upvoted 3 times

  **UFanat** 2 years, 2 months ago

Selected Answer: D

DoS protection profile should be used

upvoted 2 times

  **FS68** 2 years, 11 months ago

D is correct

upvoted 2 times

  **tech_catarina_mall** 4 years ago

Updated link:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules/dos-protection-profiles.html>

upvoted 2 times

Which two methods can be used to verify firewall connectivity to AutoFocus? (Choose two.)

- A. Verify AutoFocus status using the CLI `test` command.
- B. Check the WebUI Dashboard AutoFocus widget.
- C. Check for WildFire forwarding logs.
- D. Check the license.
- E. Verify AutoFocus is enabled below Device Management tab.

Correct Answer: DE

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/getting-started/enable-autofocus-threat-intelligence>



  **jeremykebir** 2 months, 1 week ago

Sorry to all of you, but only A & B check the well connectivity with Auto Focus :)
Good luck
upvoted 1 times


  **Marshpillowz** 7 months, 1 week ago

Selected Answer: DE

D and E appear to be correct
upvoted 1 times

  **secdaddy** 1 year, 11 months ago

A seems possible if one has the destination IP information but would only check L3/L4
Why not B? For example the autofocus dashboard alerts widget which presumably wouldn't have any alerts if the firewall were not connected to autofocus?
<https://docs.paloaltonetworks.com/autofocus/autofocus-admin/autofocus-alerts/view-alerts-in-autofocus#id988b3d9f-7526-4ec6-9ece-e7e4e70b6156>
C these logs are presumably not visible to us as they're PAN cloud to PAN cloud?
D seems this would only confirm firewall to portal connectivity for license activation
E doesn't check connectivity
Overall a poorly worded question. I agree DE are steps to connecting and are maybe best but maybe AB are possible to actually 'verify connectivity' ?
upvoted 3 times

  **Knowledge33** 1 year, 3 months ago

license is the most important. You can't use AutoFocus without license.
upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: DE

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/threat-prevention/learn-more-about-and-assess-threats/assess-firewall-artifacts-with-autofocus/enable-autofocus-threat-intelligence#id9ac4f191-abbf-4483-8a43-57bc137038ce>
upvoted 2 times



  **GivemeMoney** 2 years, 7 months ago

Seems this question may be outdated

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/threat-prevention/learn-more-about-and-assess-threats/assess-firewall-artifacts-with-autofocus/enable-autofocus-threat-intelligence.html>

steps 1 and 2 describe D and E to enable autofocus.

steps 4 is the answer: "Test the connection between the firewall and AutoFocus.:
-On the firewall, select Monitor>Logs>Traffic.
-Verify that you can Assess Firewall Artifacts with AutoFocus."
But no answers to select for those...
upvoted 3 times


  **fatespb** 2 years, 11 months ago

I would prefer A and E.
upvoted 2 times

  **Elvenking** 2 years, 4 months ago

test commands are used to verify whether a particular traffic would pass, get blocked or finally how it would be recognized by the firewall. I think "test" would a last resort and out of scope.

upvoted 1 times

 **jordan_gsi** 3 years, 5 months ago

DE

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/learn-more-about-and-assess-threats/assess-firewall-artifacts-with-autofocus/enable-autofocus-threat-intelligence.html>

upvoted 4 times

Which CLI command enables an administrator to check the CPU utilization of the dataplane?

- A. show running resource-monitor
- B. debug data-plane dp-cpu
- C. show system resources
- D. debug running resources

Correct Answer: A

trashboat Highly Voted 3 years, 4 months ago

A is the correct answer.

'show running resource-monitor' shows Dataplane CPU statistics

'show system resources [follow]' shows Management CPU statistics

upvoted 13 times

MS_NW Highly Voted 4 years, 1 month ago

Looks A

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CluDCAS>

upvoted 11 times

Marshpillowz Most Recent 7 months, 1 week ago

Selected Answer: A

Correct answer is A

upvoted 1 times

Knowledge33 1 year, 3 months ago

Selected Answer: A

This is the output from a PAN:

```
admin@palo-1> show running resource-monitor
```

Resource monitoring sampling data (per second):

CPU load sampling by group:

flow_lookup : 2%

flow_fastpath : 2%

flow_slowpath : 2%

flow_forwarding : 2%

flow_mgmt : 2%

flow_ctrl : 2%

nac_result : 0%

flow_np : 2%

upvoted 2 times

TAKUM1y 1 year, 11 months ago

Selected Answer: A

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRTCA0>

upvoted 1 times

lol1000 3 years, 10 months ago

a

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRTCA0>

upvoted 2 times

teenvignesh 4 years ago

Answer - A

upvoted 1 times

Which DoS protection mechanism detects and prevents session exhaustion attacks?

- A. Packet Based Attack Protection
- B. Flood Protection
- C. Resource Protection
- D. TCP Port Scan Protection

Correct Answer: C

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules/dos-protection-profiles>

  **lol1000** Highly Voted 3 years, 10 months ago

C

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules/dos-protection-profiles.html>

upvoted 8 times

  **rammsdoct** Highly Voted 4 years, 2 months ago

Just to clarify, C: correct

<https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/policy/security-profiles/dos-protection-profiles>



upvoted 8 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: C


C is correct

upvoted 1 times

  **NTGuru** 8 months, 1 week ago

In addition to setting IP flood thresholds, you can also use DoS Protection profiles to detect and prevent session exhaustion attacks in which a large number of hosts (bots) establish as many sessions as possible to consume a target's resources. On the profile's Resources Protection tab, you can set the maximum number of concurrent sessions that the device(s) defined in the DoS Protection policy rule to which you apply the profile can receive. When the number of concurrent sessions reaches its maximum limit, new sessions are dropped.

upvoted 1 times

  **gc999** 10 months, 1 week ago

Just wonder why the answer is not "B". I see the question is prevent "attack". So if Resources Protection, it will limit the concurrent connections including legitimate traffic.

If the question is without the word "attack", then I will choose C.



upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules/dos-protection-profiles#ida42d52fa-3366-4695-bb4a-d39ebf3b6a5f>



upvoted 1 times

  **eyelasers1** 2 years, 6 months ago

C. In addition to setting IP flood thresholds, you can also use DoS Protection profiles to detect and prevent session exhaustion attacks in which a large number of hosts (bots) establish as many sessions as possible to consume a target's resources. On the profile's Resources Protection tab, you can set the maximum number of concurrent sessions that the device(s) defined in the DoS Protection policy rule to which you apply the profile can receive. When the number of concurrent sessions reaches its maximum limit, new sessions are dropped.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules/dos-protection-profiles.html>

upvoted 2 times

  **evdw** 3 years, 4 months ago



Correct Answer: C

upvoted 1 times

  **achille5** 3 years, 5 months ago

Correct answer is C

upvoted 1 times



  **SB13** 3 years, 7 months ago

CORRECTION:

In addition to setting IP flood thresholds, you can also use DoS Protection profiles to detect and prevent session exhaustion attacks

Answer is C

upvoted 3 times

  **SB13** 3 years, 7 months ago


It is asking for which "mechanism" . Is the answer not B?

upvoted 2 times

  **myname_1** 1 year, 8 months ago

In the DoS protection profile, Flood Protection is separate from Resource Protection. Resource Protection allows you to specify the max number of concurrent sessions.

upvoted 1 times

  **GivemeMoney** 2 years, 7 months ago

It is C not B.

In addition to setting IP flood thresholds, you can also use DoS Protection profiles to detect and prevent session exhaustion attacks in which a large number of hosts (bots) establish as many sessions as possible to consume a target's resources. On the profile's Resources Protection tab, you can set the maximum number of concurrent sessions that the device(s) defined in the DoS Protection policy rule to which you apply the profile can receive. When the number of concurrent sessions reaches its maximum limit, new sessions are dropped.

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules/dos-protection-profiles.html>

upvoted 2 times

Which two subscriptions are available when configuring Panorama to push dynamic updates to connected devices? (Choose two.)

- A. Content-ID
- B. User-ID
- C. Applications and Threats
- D. Antivirus

Correct Answer: CD

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-dynamic-updates>

  **zhawk7661** Highly Voted 4 years, 1 month ago

ANSWER: C,D

upvoted 15 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: CD

C and D appear to be most correct here


upvoted 1 times

  **myname_1** 1 year, 8 months ago

The answer is still C and D, but subscription ≠ license.

Subscriptions are the Dynamic Update sections, which are App and Threats, Antivirus, Wildfire, and technically Global Protect

upvoted 2 times

  **secdaddy** 1 year, 11 months ago

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/upgrade-panorama/deploy-updates-to-firewalls-log-collectors-and-wildfire-appliances-using-panorama/supported-updates>

No mention of either Content-ID or User-ID leaves only CD as possible answers

upvoted 2 times

  **JMIB** 2 years ago

ANSWER: C,D

upvoted 1 times

  **Pretorian** 2 years, 1 month ago

FYI "Antivirus" is NOT a subscription. It is part of the Threat prevention subscription.

Therefore this question and the answers are messed up. Which is not uncommon for PANW tests.

upvoted 1 times

  **Pretorian** 2 years, 1 month ago

Applications and threats is correct, nothing else in the answers because antivirus is not a subscription

upvoted 1 times

View the GlobalProtect configuration screen capture.

What is the purpose of this configuration?

The screenshot shows the 'Configs' section of the Palo Alto Networks GlobalProtect configuration. The 'Internal' tab is active. Under the 'Internal Host Detection IPv4' section, the checkbox is checked. The IP Address field is set to '192.168.10.1' and the Hostname field is set to 'host.my.domain'. The 'Internal Host Detection IPv6' section is also visible but its checkbox is unchecked.

- A. It configures the tunnel address of all internal clients to an IP address range starting at 192.168.10.1.
- B. It forces an internal client to connect to an internal gateway at IP address 192.168.10.1.
- C. It enables a client to perform a reverse DNS lookup on 192.168.10.1 to detect that it is an internal client.
- D. It forces the firewall to perform a dynamic DNS update, which adds the internal gateway's hostname and IP address to the DNS server.

Correct Answer: C

Reference:

<https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/globalprotect-portals/define-the-globalprotect-client-authentication-configurations/define-the-globalprotect-agent-configurations>

Marshpillowz 7 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

TAKUM1y 1 year, 11 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-portals/define-the-globalprotect-app-configurations>

upvoted 2 times

UFanat 2 years, 2 months ago

Selected Answer: C

C. Reverse DNS lookup should be done to check Internal network.

upvoted 2 times

FS68 2 years, 11 months ago

C is correct

upvoted 2 times

evdw 3 years, 4 months ago

correct answer : C

upvoted 3 times

shetoshandasa 3 years, 5 months ago

"C" is correct

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/globalprotect/network-globalprotect-portals/globalprotect-portals-agent-configuration-tab/globalprotect-portals-agent-internal-tab>

upvoted 3 times

Which three user authentication services can be modified to provide the Palo Alto Networks NGFW with both usernames and role names? (Choose three.)

- A. TACACS+
- B. Kerberos
- C. PAP
- D. LDAP
- E. SAML
- F. RADIUS

Correct Answer: AEF

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication>

  **ChiaPet75** Highly Voted 4 years, 2 months ago

Correct: A,E,F

The administrative accounts are DEFINED on an external SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall.

Kerberos, LDAP, and PAP required the admin account to be locally defined on the firewall.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication.html>

upvoted 20 times

  **Edu147** Highly Voted 5 years, 1 month ago

Correct: A, E, F

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication#>

upvoted 9 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: AEF

A, E and F correct

upvoted 1 times

  **darcone23** 6 months, 1 week ago

you can use LDAP too

upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: AEF

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication>

upvoted 1 times

  **UFanat** 2 years, 2 months ago



Selected Answer: AEF

A E F

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication>

Only AEF can map roles from external auth services. Other requires to manage roles locally on the firewall.



upvoted 2 times

  **KAAC** 4 years, 1 month ago

A,E,F

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication>

upvoted 3 times

  **oo7** 4 years, 4 months ago

AEF

Central management of account authorization (role and access domain assignments). SAML, TACACS+, and RADIUS support this option for administrators.

more info

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/authentication/authentication-types/external-authentication-services.html>

upvoted 2 times

  **asmaam** 4 years, 5 months ago

Correct ans = AEF

upvoted 2 times

Question #102

Topic 1

What is exchanged through the HA2 link?

- A. hello heartbeats
- B. User-ID information
- C. session synchronization
- D. HA state information

Correct Answer: C

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/high-availability/ha-concepts/ha-links-and-backup-links>

  **ChiaPet75** Highly Voted 4 years, 2 months ago

Correct: C

"Data Link—The HA2 link is used to synchronize sessions, forwarding tables, IPSec security associations and ARP tables between devices in an HA pair. Data flow on the HA2 link is always unidirectional (except for the HA2 keep-alive); it flows from the active device to the passive device."

<https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-aws/high-availability-for-vm-series-firewall-on-aws/ha-links#:~:text=%E2%80%94The%20HA1%20link%20is%20used,port%20is%20used%20for%20HA1.>

upvoted 13 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: C

Correct answer is C

upvoted 1 times


  **[Removed]** 11 months ago

Selected Answer: C

The HA2 link is used to synchronize sessions, forwarding tables, IPSec security associations and ARP tables between firewalls in an HA pair. Data flow on the HA2 link is always unidirectional (except for the HA2 keep-alive); it flows from the active or active-primary firewall to the passive or active-secondary firewall. The HA2 link is a Layer 2 link, and it uses ether type 0x7261 by default.

Ports used for HA2—The HA data link can be configured to use either IP (protocol number 99) or UDP (port 29281) as the transport, and thereby allow the HA data link to span subnets.

upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/ha-links-and-backup-links>

upvoted 1 times

  **NatiCare** 3 years, 7 months ago

correct is C

upvoted 3 times

Which prerequisite must be satisfied before creating an SSH proxy Decryption policy?

- A. Both SSH keys and SSL certificates must be generated.
- B. No prerequisites are required.
- C. SSH keys must be manually generated.
- D. SSL certificates must be generated.

Correct Answer: B

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssh-proxy>

  **MyWil** Highly Voted 4 years, 1 month ago

Per the Palo Alto URL provided:

Configuring SSH Proxy does not require certificates and the key used to decrypt SSH sessions is generated automatically on the firewall during boot up.

With SSH decryption enabled, all SSH traffic identified by the policy is decrypted and identified as either regular SSH traffic or as SSH tunneled traffic. SSH tunneled traffic is blocked and restricted according to the profiles configured on the firewall. Traffic is re-encrypted as it exits the firewall.

Answer B is correct.

upvoted 21 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssh-proxy>

upvoted 3 times

  **UFanat** 2 years, 2 months ago

Selected Answer: B

No prereq for SSH proxy

upvoted 1 times

A customer wants to combine multiple Ethernet interfaces into a single virtual interface using link aggregation. Which two formats are correct for naming aggregate interfaces? (Choose two.)

- A. ae.8
- B. aggregate.1
- C. ae.1
- D. aggregate.8

Correct Answer: AC

  **zhawk7661** Highly Voted 4 years, 1 month ago

Correct Answer: AC
upvoted 9 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: AC

A and C are correct
upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago



Selected Answer: AC

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/network/network-interfaces/aggregate-ethernet-ae-interface-group>
upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: AC

Correct Answer: AC
upvoted 1 times

  **Gabuu** 2 years, 7 months ago

A and C are correct

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/network/network-interfaces/aggregate-ethernet-ae-interface-group.html>
upvoted 2 times

  **Questionario** 3 years, 6 months ago

I guess AC but none are correct because the dot would be for subinterfaces on the aggregate... still the aggregate would be numbered... e.g. ae1 and ae8 would be valid
upvoted 4 times

Which three authentication factors does PAN-OS® software support for MFA? (Choose three.)

- A. Push
- B. Pull
- C. Okta Adaptive
- D. Voice
- E. SMS

Correct Answer: ADE

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-multi-factor-authentication>

▣  **zhawk7661** Highly Voted 4 years, 1 month ago

Correct Answer: ADE
upvoted 7 times


▣  **evdw** Highly Voted 3 years, 4 months ago

Correct answer : A, D, E
upvoted 5 times

▣  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: ADE

A, D and E are correct
upvoted 1 times

▣  **Sarbi** 1 year, 8 months ago

ADE is correct one
upvoted 1 times

▣  **TAKUM1y** 1 year, 11 months ago

Selected Answer: ADE

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/authentication/authentication-types/multi-factor-authentication>
upvoted 4 times

▣  **NatiCare** 3 years, 7 months ago

A,D,E
<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/authentication-types/multi-factor-authentication>
upvoted 4 times

▣  **UmaShankar** 3 years, 10 months ago

correct ADE
upvoted 4 times

VPN traffic intended for an administrator's firewall is being maliciously intercepted and retransmitted by the interceptor. When creating a VPN tunnel, which protection profile can be enabled to prevent this malicious behavior?

- A. Zone Protection
- B. Replay
- C. Web Application
- D. DoS Protection

Correct Answer: B

  **Pretorian** Highly Voted  2 years ago

Terrible question as usual with PANW tests. There is no "Replay protection profile" this is a checkbox in the IPsec tunnel creation part (-_-)...
upvoted 12 times

  **Marshpillowz** Most Recent  7 months, 1 week ago

Selected Answer: B

B is correct
upvoted 1 times

  **Merlin0o** 1 year ago

Selected Answer: B

B
"If you choose Auto Key, specify the following:"

"Enable Replay Protection—Select to protect against replay attacks.

The anti-replay protocol is used to prevent hackers from injecting or making changes in packets that travel from a source to a destination and uses a unidirectional security association in order to establish a secure connection between two nodes in the network."

Src:

<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/network/network-ipsec-tunnels/ipsec-tunnel-general-tab>
upvoted 2 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/network/network-ipsec-tunnels/ipsec-tunnel-general-tab>
upvoted 2 times

  **JMIB** 2 years ago

Correct is B
upvoted 1 times

  **eyelasers1** 2 years, 6 months ago

B.
<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/network/network-ipsec-tunnels/ipsec-tunnel-general-tab.html>
upvoted 3 times

Which Zone Pair and Rule Type will allow a successful connection for a user on the Internet zone to a web server hosted on the DMZ zone? The web server is reachable using a Destination NAT policy in the Palo Alto Networks firewall.

A.

Zone Pair:

Source Zone: Internet

Destination Zone: Internet

Rule Type:

'intrazone'

B.

Zone Pair:

Source Zone: Internet

Destination Zone: DMZ

Rule Type:

'interzone' or 'universal'

C.

Zone Pair:

Source Zone: Internet

Destination Zone: Internet

Rule Type:

'intrazone' or 'universal'

D.

Zone Pair:

Source Zone: Internet

Destination Zone: DMZ

Rule Type:

'intrazone'

Correct Answer: B

  **kraut**  3 years, 4 months ago

B

everything EXCEPT destination zone is pre-nat

pre-nat dest ip, post-nat dest zone

upvoted 11 times

  **mtberdaan** 3 years, 2 months ago

Yes answer will be B, but the zone is correct DMZ is the post-nat destination zone;

the NAT rule will look like this:

source zone: Internet

destination zone: Internet

destination IP: public IP

destination translation: internal IP

the SEC rule will look like this:

source zone: Internet

destination zone: DMZ (post-NAT)

destination IP: Public IP (pre-NAT)

Which will make the traffic interzone.

Tip:



interzone vs intrazone -- I think of internet (global) vs intranet (local)

upvoted 11 times

  **keto3812**  3 years, 5 months ago



Question is ambiguous. is it looking for NAT rule or Security Policy Rule?

upvoted 7 times

  **kraut** 3 years, 4 months ago

It states that there is a NAT rule in place, so we're looking for the security policy.

upvoted 2 times

  **vj77** 3 years, 4 months ago

it could also be interpreted as there is a NAT policy in place, what should it be?

upvoted 2 times

  **lildevil** 1 year, 2 months ago



The question asks "allow a successful connection" NAT policies do not allow traffic, Sec policies do.

upvoted 2 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

B is correct

upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

B. Pre Nat IP and Post NAT zone.

upvoted 3 times

  **TAKUM1y** 1 year, 11 months ago

B → <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomCAC>

upvoted 3 times

  **GivemeMoney** 2 years, 7 months ago

the only difference between B and D is - B has a rule type of: interzone or universal, and D only has a rule type of interzone. What's the difference?

upvoted 1 times

  **GivemeMoney** 2 years, 7 months ago

found it: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomCAC>

By default, all the traffic destined between two zones, regardless of being from the same zone or different zone, this applies the rule to all matching interzone and intrazone traffic in the specified source and destination zones.

upvoted 1 times



An administrator has configured a QoS policy rule and a QoS Profile that limits the maximum allowable bandwidth for the YouTube application. However, YouTube is consuming more than the maximum bandwidth allotment configured. Which configuration step needs to be configured to enable QoS?

- A. Enable QoS interface
- B. Enable QoS in the Interface Management Profile
- C. Enable QoS Data Filtering Profile
- D. Enable QoS monitor

Correct Answer: A

  **Ab121213** Highly Voted 4 years, 3 months ago

QoS implementation on a Palo Alto Networks firewall begins with three primary configuration components that support a full QoS solution: a QoS policy, a QoS Profile, and configuration of the QoS egress interface.
study guide page 225
upvoted 15 times

  **rammsdoct** Highly Voted 4 years, 2 months ago
agreed on A:

you create policy rule but still not being applied on the outbound/inbound interface
upvoted 6 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: A

Weird wording but correct answer is A
upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/quality-of-service/configure-qos>
upvoted 3 times

  **trashboat** 3 years, 4 months ago

A is correct, and I agree with Daniel.
This is confusing wording though, you don't enable a special QoS interface, you enable QoS [on an] interface.
upvoted 3 times

  **Chris71Mach1** 1 year, 7 months ago

This is exactly what threw me off with this question. I hate how exams seem to almost intentionally misword questions to trip folks up just to lower exam scores.
upvoted 1 times

  **Daniel2020** 3 years, 10 months ago

A

You can find this answer in the PCNSE Study Guide (August 2020 version on page 257) study guide or the PAN-OS guide here
Reference <https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/quality-of-service/configure-qos.html>
upvoted 3 times

Which log file can be used to identify SSL decryption failures?

- A. Traffic
- B. ACC
- C. Configuration
- D. Threats

Correct Answer: A

Daniel2020 Highly Voted 3 years, 10 months ago

A

Always from the traffic log. Whether it is drilling down into traffic log details or enabling the decryption column.

Acquaint yourself with this reference:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/verify-decryption.html>

upvoted 9 times

Micutzu Highly Voted 10 months ago

Selected Answer: A

The question is about "log file" and SSL decrypt failures. ACC isn't a log file.

SLL decrypt failures you can see on Decryption log and in Traffic log (Session End Reason column)

upvoted 6 times

Od2fdfa Most Recent 3 months, 3 weeks ago

Selected Answer: B

B is correct according to the documentation.

The most common reasons for decryption failures are TLS protocol errors, cipher version errors (client and server version mismatches and client and Decryption profile version mismatches), and certificate errors. To investigate decryption errors, start with the Application Command Center (ACC) to identify failures and then go to the Decryption logs to drill down into details.

Option is is Traffic and NOT "Decryption logs"

<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/decryption/troubleshoot-and-monitor-decryption/decryption-troubleshooting-workflow-examples/investigate-decryption-failure-reasons>

upvoted 1 times

327c7c8 5 months, 1 week ago

B: Is the correct answer.

ACC>SSL Activity>Decryption failure reasons

Give you the information about the failure.

Traffic log can you verify if the traffic is encrypted or not.

There are no details about the failure.

upvoted 3 times

Marshpillowz 7 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

news088 1 year ago

ACC is not a log file . The question is about "Which log file", so A should be the correct one.

upvoted 1 times

duckduckgoo 1 year, 3 months ago

Selected Answer: B

I am going to go with B

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/troubleshoot-and-monitor-decryption/decryption-troubleshooting-workflow-examples/investigate-decryption-failure-reasons>

What people are selecting is for validating if decryption was used, but not for specific failures.

upvoted 2 times

PaloSteve 1 year, 1 month ago

From this article: "To investigate decryption errors, start with the Application Command Center (ACC) to identify failures and then go to the Decryption logs to drill down into details."

So, the real answer might be the Decryption logs, which, of course, is not an option. LOL.

upvoted 2 times

  **DenskyDen** 1 year, 7 months ago

Selected Answer: A

View Decrypted Traffic Sessions—Filter the Traffic Logs (MonitorLogsTraffic) using the filter (flags has proxy)
<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/verify-decryption#id185BG0KL0W1>
upvoted 1 times

  **PaloSteve** 1 year, 1 month ago

This flag is only for traffic that has been successfully decrypted. It will not help identify SSL decryption failures
upvoted 2 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/verify-decryption>
upvoted 2 times

  **Pretorian** 2 years ago



Another tricky question, very common with PANW tests.

While I agree with "A", if you go to "Monitor > Decryption" you will see an "Error" and "Error Index" column (if you don't see it, you can enable it).



The Traffic log will only tell you if a session was decrypted or not, but no-decrypted traffic doesn't always mean a failure, it could often mean there's a decryption policy with action "no decrypt" or an SSL decryption exclusion or an error.

Something to think about...

upvoted 1 times



  **FS68** 2 years, 11 months ago

A because ACC isn't a log file
upvoted 2 times

  **kike71** 3 years, 2 months ago

I think that correct answer is B
PANOS Guide. Investigate Decryption Failure Reasons
Begin your investigation at ACC>SSL Activity and look at the Decryption Failure Reasons widget

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/troubleshoot-and-monitor-decryption/decryption-troubleshooting-workflow-examples/investigate-decryption-failure-reasons.html#id1eee110d-3799-45ef-a4b0-e5e7fbd157af>
upvoted 2 times

  **kike71** 3 years, 2 months ago

There is a thing that dizzies me... ACC isn't a log file
upvoted 2 times

  **duckduckgoo** 1 year, 5 months ago

Dang it, I gotta read slower. I was looking why it wasn't that since 10.x has that great feature.
upvoted 1 times

  **thegreek1** 3 years, 2 months ago

Confirmed that the answer is A Traffic.

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/verify-decryption.html>
upvoted 3 times

  **kraut** 3 years, 4 months ago

IMHO: A - traffic log

specifically check session end reason where decrypted=yes and action=allowed. you'll see errors such as
decrypt-error
decrypt-cert-validation



upvoted 2 times

  **lucaboban** 3 years, 5 months ago

The following tools provide full visibility into the TLS handshake and help you troubleshoot and monitor your decryption deployment:
ACC - SSL Activity
Monitor - Logs - Decryption
So as there is no Decryption listed as answer, ACC fits.

Correct answer is: A

upvoted 1 times

  **CKPH** 3 years, 6 months ago

PCNSE is based on PANOS10
<https://live.paloaltonetworks.com/t5/certification-articles/pcnse-and-pcnsa-exam-changes-with-10-0/ta-p/344832>
Could be B:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-release-notes/pan-os-10-0-release-information/features-introduced-in-pan-os-10-0/decryption-features.html#ida1eb9d8c-515e-4e88-b217-1ebc025a45d4>

"Use the new ACC features to identify traffic for which decryption causes problems and then use the new Decryption logs to drill down into details and solve the problem."

upvoted 1 times

  **Prutser2** 3 years, 2 months ago

agree could be, again wording of question, clearly states "log file" ACC is not a log file. so brings back to A

upvoted 1 times

  **Daniel2020** 3 years, 7 months ago

B - as from PAN-OS 10, troubleshooting SSL is done in the following process:

1. Check ACC decryption widgets to identify traffic that causes decryption issues
2. Drill down further using the Decryption Log.

It is not A because that simply tells you if the traffic was or was not decrypted. It does not in any way provide you with a means for troubleshooting. The question is asking you to troubleshoot.

Read "Troubleshoot and Monitor Decryption" for PAN-OS 10. It clearly lists your troubleshooting process for SSL decryption issues

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/troubleshoot-and-monitor-decryption.html>

upvoted 3 times

  **bmarks** 3 years, 6 months ago

The Question is simply asking which 'log file' lists/identifies decrypt failures, not how and where do I troubleshoot them... The Application Command Center (ACC) is an analytical tool, not a log file. The only answer that makes sense is A Traffic log.

upvoted 4 times

  **bmarks** 3 years, 6 months ago

Also, the PCNSE 9 exam covers PANOS 9.1, not PANOS 10

upvoted 1 times

A customer wants to set up a site-to-site VPN using tunnel interfaces.
Which two formats are correct for naming tunnel interfaces? (Choose two.)

- A. tunnel.1
- B. vpn-tunnel.1
- C. tunnel.1025
- D. vpn-tunnel.1024

Correct Answer: AC

  **zhawk7661** Highly Voted 4 years, 1 month ago

Correct Answer: AC
upvoted 9 times

  **Ditzhak** Most Recent 5 months, 3 weeks ago

A and C are both correct
upvoted 1 times


  **Marshpillowz** 7 months, 1 week ago

Selected Answer: AC

A and C are correct
upvoted 1 times



  **DenskyDen** 1 year, 7 months ago

AC. 100%
upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: AC

A & C are correct
upvoted 2 times

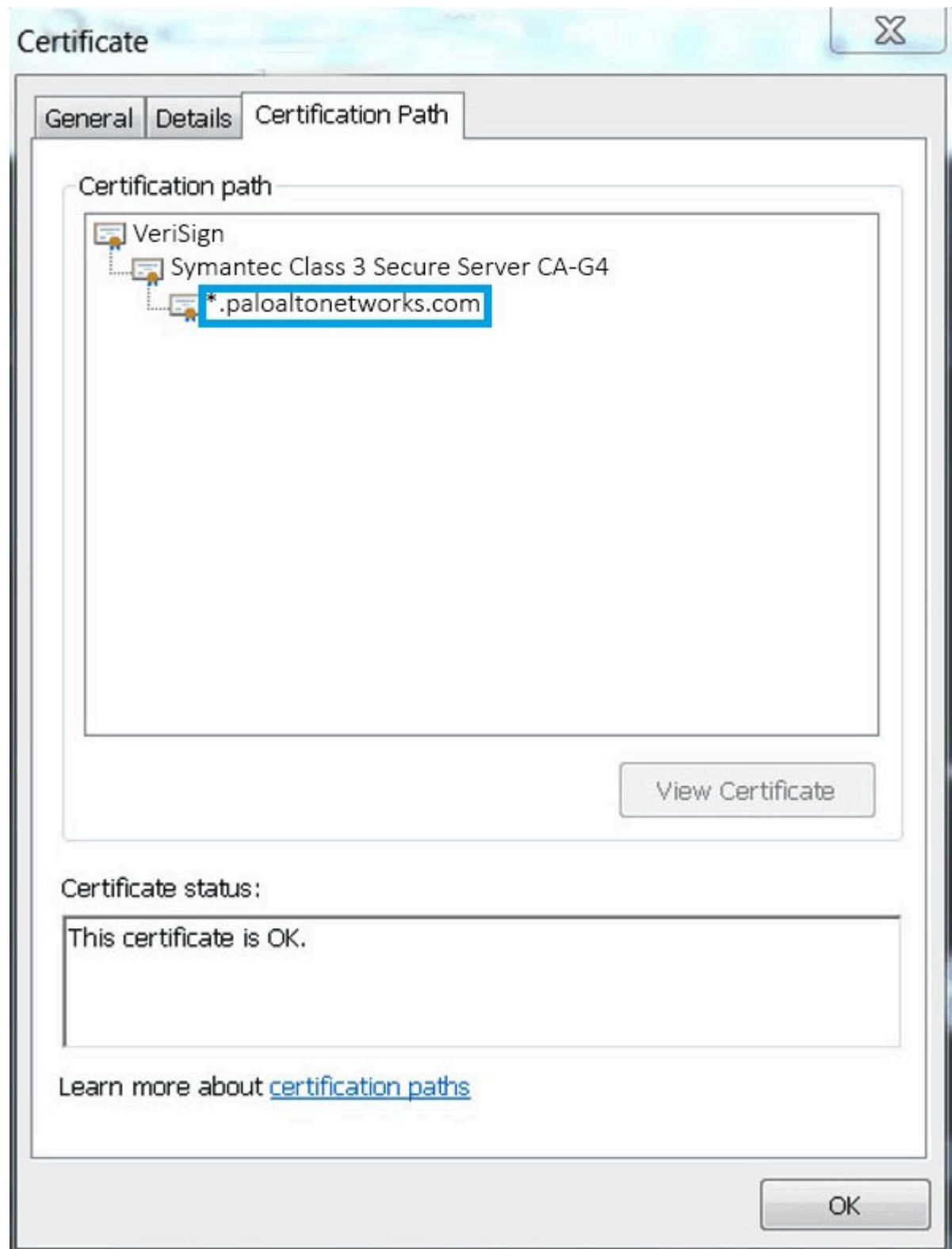
  **Gabuu** 2 years, 7 months ago

A and C
upvoted 3 times

  **sabrimalik** 3 years, 1 month ago

Correct answer is AC
upvoted 3 times

Based on the following image, what is the correct path of root, intermediate, and end-user certificate?



- A. Palo Alto Networks > Symantec > VeriSign
- B. VeriSign > Symantec > Palo Alto Networks
- C. Symantec > VeriSign > Palo Alto Networks
- D. VeriSign > Palo Alto Networks > Symantec

Correct Answer: B

Meira088 Highly Voted 2 years, 3 months ago

Selected Answer: B

b the correct answer
upvoted 5 times

Marshpillowz Most Recent 7 months, 1 week ago

Selected Answer: B

B is correct
upvoted 1 times

fireb 2 years, 3 months ago

Obviously B
upvoted 3 times

Elvenking 2 years, 4 months ago

This question is tricky, as it seems to ask "according to the exhibit" what is the path... but to be relevant to PCNSE the question may be asking "what is the correct way to make a chained certificate?".

The answer should be A:

First attach the final certificate, then add the signer thereof and follow it by the signing root authority. This is correct according to:
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClkoCAC>

upvoted 3 times

  **DatITGuyTho1337** 8 months, 2 weeks ago

I agreed with you until I read the latter part of the question that literally asked what the root, intermediate and end-user certificate would be. B answers that out right.

upvoted 1 times

  **confusion** 2 years, 6 months ago

Selected Answer: B



Only B

upvoted 2 times

  **pabartur** 2 years, 7 months ago

Selected Answer: B


upvoted 2 times

  **obas** 2 years, 7 months ago

Selected Answer: B

B is correct



upvoted 3 times

  **Imla89** 2 years, 8 months ago

Selected Answer: B

B is correct


upvoted 3 times

  **kolz** 2 years, 9 months ago

Selected Answer: B

B is correct

upvoted 2 times

  **FS68** 2 years, 11 months ago



B is correct

upvoted 2 times

  **yogininangpal** 3 years, 3 months ago


It should be B

upvoted 2 times

  **Qintao** 3 years, 4 months ago


absolutely B.

upvoted 2 times

  **frodo1791** 3 years, 4 months ago

It should be option B.

upvoted 3 times

  **Adamabdi** 3 years, 4 months ago



B is correct

upvoted 3 times

  **lucaboban** 3 years, 5 months ago

B seems to be correct path IMO

upvoted 3 times

  **bloodtech** 3 years, 5 months ago

Should be B ?

upvoted 4 times

  **VivekSL512** 3 years, 5 months ago

Yes it seems should be "B" > Verisign > Symantec > Palo Alto

upvoted 5 times

An administrator wants a new Palo Alto Networks NGFW to obtain automatic application updates daily, so it is configured to use a scheduler for the application database. Unfortunately, they required the management network to be isolated so that it cannot reach the Internet. Which configuration will enable the firewall to download and install application updates automatically?

- A. Download and install application updates cannot be done automatically if the MGT port cannot reach the Internet.
- B. Configure a service route for Palo Alto Networks Services that uses a dataplane interface that can route traffic to the Internet, and create a Security policy rule to allow the traffic from that interface to the update servers if necessary.
- C. Configure a Policy Based Forwarding policy rule for the update server IP address so that traffic sourced from the management interfaced destined for the update servers goes out of the interface acting as your Internet connection.
- D. Configure a Security policy rule to allow all traffic to and from the update servers.

Correct Answer: B

  **zhawk7661** Highly Voted 4 years, 1 month ago

Correct Answer: B
upvoted 11 times



  **Acidscars** 3 years, 6 months ago

Agree. Service Route will solve this problem. B
upvoted 3 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: B

B is correct
upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/service-routes>
upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/service-routes/service-routes-overview>
upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: B

If management port cannot reach the Internet you should manually configure service routes
upvoted 2 times

  **fireb** 2 years, 3 months ago

B is correct.
upvoted 2 times

A company wants to install a NGFW firewall between two core switches on a VLAN trunk link. They need to assign each VLAN to its own zone and to assign untagged (native) traffic to its own zone.

Which option differentiates multiple VLANs into separate zones?

- A. Create V-Wire objects with two V-Wire interfaces and define a range of $\lambda\epsilon 0-4096\lambda\epsilon$ in the $\lambda\epsilon\text{Tag Allowed}\lambda\epsilon$ field of the V-Wire object.
- B. Create V-Wire objects with two V-Wire subinterfaces and assign only a single VLAN ID to the $\lambda\epsilon\text{Tag Allowed}\lambda\epsilon$ field of the V-Wire object. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each interface/subinterface to a unique zone.
- C. Create Layer 3 subinterfaces that are each assigned to a single VLAN ID and a common virtual router. The physical Layer 3 interface would handle untagged traffic. Assign each interface/subinterface to a unique zone. Do not assign any interface an IP address.
- D. Create VLAN objects for each VLAN and assign VLAN interfaces matching each VLAN ID. Repeat for every additional VLAN and use a VLAN ID of 0 for untagged traffic. Assign each interface/subinterface to a unique zone.

Correct Answer: B

  **ChiaPet75** Highly Voted 4 years, 2 months ago



Correct: B

The question says that the firewall was installed on a "trunk" link between to core switches. This mean Layer-3 is not usable in this situation.

"Virtual wire interfaces by default allow all untagged traffic. You can, however, use a virtual wire to connect two interfaces and configure either interface to block or allow traffic based on the virtual LAN (VLAN) tags. VLAN tag 0 indicates untagged traffic.

You can also create multiple subinterfaces, add them into different zones, and then classify traffic according to a VLAN tag or a combination of a VLAN tag with IP classifiers (address, range, or subnet) to apply granular policy control for specific VLAN tags or for VLAN tags from a specific source IP address, range, or subnet."

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/configure-interfaces/virtual-wire-interfaces/vlan-tagged-traffic.html>
upvoted 21 times

  **sapahsaph** Highly Voted 3 years, 9 months ago

correct answer is B

Virtual wire interfaces by default allow all untagged traffic. You can, however, use a virtual wire to connect two interfaces and configure either interface to block or allow traffic based on the virtual LAN (VLAN) tags. VLAN tag 0 indicates untagged traffic.

You can also create multiple subinterfaces, add them into different zones, and then classify traffic according to a VLAN tag or a combination of a VLAN tag with IP classifiers (address, range, or subnet) to apply granular policy control for specific VLAN tags or for VLAN tags from a specific source IP address, range, or subnet.



upvoted 7 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: B

B is correct

upvoted 1 times

  **lol12** 1 year, 9 months ago

Selected Answer: B

Question is asking about traffic between two core switches... and this suggests VWire. In addition the requirement is for each VLAN to have it's own zone.

upvoted 2 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/configure-interfaces/virtual-wire-interfaces/virtual-wire-subinterfaces>
upvoted 2 times

  **taherborga**n 2 years, 1 month ago

answer is D

upvoted 1 times

  **Meira088** 2 years, 3 months ago

Selected Answer: B

correct answer is B



upvoted 2 times

  **tururu1496** 2 years, 6 months ago

Selected Answer: B

Answer: B (<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/networking/configure-interfaces/virtual-wire-interfaces/vlan-tagged-traffic.html>)

upvoted 2 times

  **Qintao** 3 years, 4 months ago

Bad question!

upvoted 2 times

  **webmanau** 3 years, 5 months ago

It's option B and anyone who says otherwise has probably never configured on of these firewalls. Insertion into a trunk needs vWire. C and D are plain rubbish and A does not allow individual zones. I actually set this up 7 years ago so no need to guess.

upvoted 2 times

  **shetoshandasa** 3 years, 5 months ago

Answer is "B", "C" doesn't seem to be correct because 2 layers 3 interfaces in the firewall will force you to change the g/w for all endpoints to be the FW instead of the core switch, moreover "Do not assign any interface an IP address" is another obstacle, then how will you route the traffic from the ingress port to the egress one !!

upvoted 2 times

  **lucaboban** 3 years, 5 months ago

Correct answer is C

upvoted 1 times

  **GivemeMoney** 2 years, 7 months ago

Explain why?

upvoted 2 times

  **bmarks** 3 years, 6 months ago

Best Answer = B Based on PAN Documentation on Virtual Wire Subinterfaces:

Virtual wire deployments can use virtual wire subinterfaces to separate traffic into zones.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/configure-interfaces/virtual-wire-interfaces/virtual-wire-subinterfaces.html>

C is L3 subinterfaces that will require an IP address to pass traffic

upvoted 4 times

  **DocHoliday** 3 years, 7 months ago

c can't be correct layer 3 always needs an IP



upvoted 1 times

  **NatiCare** 3 years, 7 months ago

The correct is D,

C is layer 3.

upvoted 2 times

  **duyvo** 3 years, 7 months ago



Ans is D.

A. Define a range of "0-4096" will allow all VLAN pass through the vWire but can not separate zones.

B. Can not assign VLAN ID to the "Tag Allowed" of V-Wire subinterfaces

C. Layer 3 subinterfaces can not link between two physical interface unless use vWire subinterfaces or Layer 2 subinterfaces

upvoted 1 times

  **Sarbi** 3 years, 9 months ago

C is correct.

upvoted 1 times

Which data flow describes redistribution of user mappings?

- A. User-ID agent to firewall
- B. Domain Controller to User-ID agent
- C. User-ID agent to Panorama
- D. firewall to firewall

Correct Answer: D


- [-] **CiscoNinja** Highly Voted 4 years, 3 months ago
D - Firewall to firewall or Firewall to Panorama
upvoted 13 times
- [-] **cipri86** Highly Voted 3 years, 7 months ago
D - Firewall to Firewall
<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/deploy-user-id-in-a-large-scale-network/redistribute-user-mappings-and-authentication-timestamps/firewall-deployment-for-user-id-redistribution.html#ide3661b46-4722-4936-bb9b-181679306809>
upvoted 8 times
- [-] **Marshpillowz** Most Recent 7 months, 1 week ago
Selected Answer: D
D is correct
upvoted 1 times
- [-] **ChiaPet75** 1 year ago
PCNSE Study Guide 2023 1.4.4
Firewalls share user mappings and authentication timestamps as part of the same redistribution flow; you do not have to configure redistribution separately for each information type.
upvoted 1 times
- [-] **TAKUM1y** 1 year, 11 months ago
Selected Answer: D
<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/deploy-user-id-in-a-large-scale-network/redistribute-user-mappings-and-authentication-timestamps/firewall-deployment-for-user-id-redistribution#ide3661b46-4722-4936-bb9b-181679306809>
upvoted 2 times
- [-] **UFanat** 2 years, 2 months ago
Selected Answer: D
Should be D
upvoted 2 times
- [-] **tururu1496** 2 years, 6 months ago
Selected Answer: D
Answer: D (<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/deploy-user-id-in-a-large-scale-network/redistribute-user-mappings-and-authentication-timestamps/firewall-deployment-for-user-id-redistribution.html>)
upvoted 3 times
- [-] **lmla89** 2 years, 8 months ago
Selected Answer: D
D is correct
upvoted 4 times
- [-] **fxgoat98** 3 years, 2 months ago
correct answer is D
upvoted 4 times
- [-] **GBD** 3 years, 12 months ago
A..from the PCNSE study guide revised Aug 2020
To map IP addresses to usernames, User-ID agents monitor sources such as directory servers. The agents send the user mappings to firewalls, Log Collectors, or Panorama. Each appliance then can serve as redistribution points that forward the mappings to other firewalls, Log Collectors, or Panorama. Before a firewall or Panorama can collect user mappings, you must configure its connections to the User-ID agents or redistribution points.
More information about this topic can be found here: <https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-web-interface>
upvoted 2 times

  **jpm_1506** 3 years, 8 months ago

"The agents send the user mappings to firewalls, Log Collectors, or Panorama." so far not redistribution - just collection...



then it says "Each appliance then can serve as redistribution points that forward the mappings to other firewalls, Log Collectors, or Panorama." so for it to be considered as redistribution it has to come from a firewall, panorama, or log collector. taht only leaves option "D" as an option as its the only one that sources userID from a fw, panorama ,or log collector.

upvoted 6 times

  **GBD** 3 years, 12 months ago

User-ID agent can be on a firewall or it can be on a Windows server, so I believe that the answer is A

upvoted 1 times

  **cthd** 4 years, 2 months ago

D. Redistribution supported only on FW, Log Collector, and Panorama


upvoted 1 times

  **maylinn** 4 years, 2 months ago

https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/dita/_graphics/7-1/user-id/User-ID_Redistribution.png

D is correct

upvoted 1 times

  **ChiaPet75** 4 years, 2 months ago

This one is a little confusing but I do believe that the right answer is "A".

Step 3-1 says "Configure the firewall to function as a User-ID agent.

If redistribution enables the firewall to function as a User-ID agent for other devices then the correct data flow would be "User-ID agent to firewall"

The answer is A

<https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/user-id/deploy-user-id-in-a-large-scale-network/configure-firewalls-to-redistribute-user-mapping-information/configure-user-id-redistribution.html#idc123940a-367d-4515-b45e-29c1d0aa2bd1>

In later version of the PANOS documentation it doesn't mention configuring the firewall as a User-Id agent specifically but all the configuration for redistribution is done within the User-ID agent configuration itself. See Step 1-3 in the doc link below.

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/deploy-user-id-in-a-large-scale-network/redistribute-user-mappings-and-authentication-timestamps/configure-user-id-redistribution>

upvoted 3 times

  **rammsdoct** 4 years, 3 months ago

D.

if it was collection of user ID it would be A, but instead is redistritbution.

check example below.

<https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/user-id/deploy-user-id-in-a-large-scale-network/configure-firewalls-to-redistribute-user-mapping-information/firewall-deployment-for-user-id-redistribution.html#id127bc778-ffec-49c4-a9b2-5cf7b044be6e>

upvoted 4 times

  **Ab121213** 4 years, 3 months ago

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/user-identification/device-user-identification-user-mapping/user-id-agent-setup/user-id-agent-setup-redistribution.html>

upvoted 3 times

Where can an administrator see both the management plane and data plane CPU utilization in the WebUI?

- A. System Utilization log
- B. System log
- C. Resources widget
- D. CPU Utilization widget

Correct Answer: C

  **bmarks** Highly Voted 3 years, 6 months ago

Answer = C

System Resources Widget

Displays the Management CPU usage, Data Plane usage, and the Session Count (the number of sessions established through the firewall or Panorama).

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/dashboard/dashboard-widgets.html>

upvoted 9 times

  **Ab121213** Highly Voted 4 years, 3 months ago

It is under Dashboard

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/troubleshoot-url-filtering/urls-classified-as-not-resolved.html>

upvoted 6 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/dashboard/dashboard-widgets>

upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: C

Widget for this exists

upvoted 2 times

  **confusion** 2 years, 6 months ago

Selected Answer: C

On the widget, so C.

upvoted 2 times

  **MS_NW** 4 years, 1 month ago

C

You can also view system resources on the System Resources widget on the Dashboard in the web interface.

upvoted 4 times

Which four NGFW multi-factor authentication factors are supported by PAN-OS®? (Choose four.)

- A. Short message service
- B. Push
- C. User logon
- D. Voice
- E. SSH key
- F. One-Time Password

Correct Answer: *ABDF*

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-multi-factor-authentication>

▣  **Prutser2** Highly Voted 3 years, 2 months ago

ABDF is correct answer
upvoted 6 times

▣  **eyelasers1** Highly Voted 2 years, 6 months ago


ANSWER: ABDF.
"For example, the MFA service might prompt you to select the Voice, SMS, push, or PIN code (OTP) authentication method"

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/authentication/configure-multi-factor-authentication.html>
upvoted 5 times

▣  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: ABDF

A, B, D and F correct
upvoted 1 times

▣  **DenskyDen** 1 year, 7 months ago

ABDF.
<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/authentication-types/multi-factor-authentication>
upvoted 1 times

▣  **TAKUM1y** 1 year, 11 months ago

Selected Answer: ABDF

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/authentication/authentication-types/multi-factor-authentication>
upvoted 3 times

▣  **confusion** 2 years, 6 months ago

Selected Answer: ABDF

ABDF is correct.
upvoted 3 times

Which two features does PAN-OS® software use to identify applications? (Choose two.)

- A. transaction characteristics
- B. session number
- C. port number
- D. application layer payload

Correct Answer: AD

— **LeonSKennedy** Highly Voted 4 years, 1 month ago

Answer: A,D is correct

The Palo Alto Networks firewall does not classify traffic by port and protocol; instead it identifies the application based on its unique properties and transaction characteristics using the App-ID technology. Some applications, however, require the firewall to dynamically open pinholes to establish the connection, determine the parameters for the session and negotiate the ports that will be used for the transfer of data; these applications use the application-layer payload to communicate the dynamic TCP or UDP ports on which the application opens data connections. For such applications, the firewall serves as an Application Level Gateway (ALG), and it opens a pinhole for a limited time and for exclusively transferring data or control traffic. The firewall also performs a NAT rewrite of the payload when necessary.

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/app-id/application-level-gateways#>
upvoted 26 times

— **ChiaPet75** Highly Voted 4 years, 2 months ago

Correct: A,C

"Signatures are then applied to allowed traffic to identify the application based on unique application properties and related [transaction characteristics]. The signature also determines if the application is being used on its [default port or it is using a non-standard port.] If the traffic is allowed by policy, the traffic is then scanned for threats and further analyzed for identifying the application more granularly.

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/app-id-overview.html>
upvoted 7 times

— **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: AD

A and D correct
upvoted 1 times

— **nguyendtv50** 1 year, 3 months ago

Answer: A + D
upvoted 1 times

— **DenskyDen** 1 year, 7 months ago

AD/ App-ID, a patented traffic classification system only available in Palo Alto Networks firewalls, determines what an application is irrespective of port.
upvoted 2 times

— **TAKUM1y** 1 year, 11 months ago

Selected Answer: AD

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/app-id-overview>
upvoted 2 times

— **hpbdcB** 1 year, 11 months ago

Selected Answer: AD

App-ID, a patented traffic classification system only available in Palo Alto Networks firewalls, determines what an application is irrespective of port, protocol, encryption (SSH or SSL) or any other evasive tactic used by the application.

-> notice: "irrespective of port, protocol, encryption" so A+D

Details: <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/app-id-overview>
upvoted 2 times

— **UFanat** 2 years, 2 months ago

Selected Answer: AD

Palo Alto Networks NGFW can identify app on any port with any session number
upvoted 2 times

  **1Adrian1** 2 years, 5 months ago

A and C

upvoted 2 times

  **rocioha** 3 years, 5 months ago

what means transaction characteristics?? Heuristics? why not the port?



upvoted 2 times

  **Jared28** 2 years, 6 months ago

My thought on why D instead of C - the 2nd bullet point mentions it'll identify regardless of the port and makes no mention of the port being part of the identification process. The final bullet point is what makes me think it's payload related.

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/app-id/app-id-overview.html>

upvoted 1 times

  **Mr_Cipher** 3 years, 8 months ago

A,D sounds correct

upvoted 2 times

An administrator wants to upgrade a firewall from PAN-OS® 9.1 to PAN-OS® 10.0. The firewall is not a part of an HA pair. What needs to be updated first?

- A. Applications and Threats
- B. XML Agent
- C. WildFire
- D. PAN-OS Upgrade Agent

Correct Answer: A

Marshpillowz 7 months, 1 week ago

Selected Answer: A

Correct answer is A
upvoted 1 times

mangwe263 1 year, 7 months ago

woody you failed i guess, this is the simplest question. Its A
upvoted 1 times

mine25 1 year, 8 months ago

Selected Answer: A

Step 3 from the upgrade guide: Ensure that the firewall is running the latest content release version.
upvoted 2 times

TAKUM1y 1 year, 11 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/upgrade-pan-os/upgrade-the-firewall-pan-os/upgrade-a-standalone-firewall>
upvoted 3 times

Woody 1 year, 8 months ago

Why A? This is what the above article said: "If your firewalls are configured to forward samples to a WildFire appliance for analysis, you must upgrade the WildFire appliance before upgrading the forwarding firewalls." Then that would be C.
upvoted 1 times

DenskyDen 1 year, 7 months ago

It was not mentioned on the question that firewall is configured with wildfire, so you should stick with what are the steps and step 3 is to Ensure that the firewall is running the latest content release version.
upvoted 1 times

UFanat 2 years, 2 months ago

Selected Answer: A

A. Content version should be upgraded to the required one.
upvoted 2 times

AbuHussain 2 years, 5 months ago

Selected Answer: A

Answer: A
upvoted 2 times

tururu1496 2 years, 6 months ago

Selected Answer: A

Answer: A
upvoted 2 times

confusion 2 years, 6 months ago

Selected Answer: A

Update security features first, so A.
upvoted 2 times

eyelasers1 2 years, 6 months ago

Answer: A



Ensure that the firewall is running the latest content release version.

Refer to the Release Notes for the minimum content release version you must install for a PAN-OS 10.0 release. Make sure to follow the Best Practices for Application and Threat Updates.

Select DeviceDynamic Updates and see which Applications or Applications and Threats content release version is Currently Installed.

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/upgrade-pan-os/upgrade-the-firewall-pan-os/upgrade-a-standalone-firewall.html>



upvoted 2 times

  **obas** 2 years, 7 months ago

Selected Answer: A

A is correct

upvoted 2 times

  **lmla89** 2 years, 8 months ago

Selected Answer: A

A is correct

upvoted 3 times

  **yummy_shimeji** 2 years, 8 months ago

A

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-new-features/upgrade-to-pan-os-81/upgrade-the-firewall-to-pan-os-81/upgrade-a-firewall-to-pan-os-81.html#id6d04fbd3-04c9-4180-988c-e071939646e5>

upvoted 3 times

  **Plato22** 2 years, 8 months ago

Should be A.

upvoted 4 times

When backing up and saving configuration files, what is achieved using only the firewall and is not available in Panorama?

- A. Load configuration version
- B. Save candidate config
- C. Export device state
- D. Load named configuration snapshot

Correct Answer: C

umarkhan32 Highly Voted 3 years, 11 months ago

Export device state: C
upvoted 7 times

achille5 Highly Voted 3 years, 5 months ago

C
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClgKCAS>
upvoted 6 times

z8d21oczd Most Recent 1 month, 4 weeks ago

Selected Answer: C

C seems most correct, but you can export the device state in panorama via CLI
upvoted 1 times

Marshpillowz 7 months, 1 week ago

Selected Answer: C

C is correct
upvoted 1 times

TAKUM1y 1 year, 11 months ago

Selected Answer: C

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClgKCAS>
upvoted 5 times

myname_1 1 year, 8 months ago

Sort of the same idea, but this article is better because it isn't a loaded question:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRcCAK>
upvoted 1 times

UFanat 2 years, 2 months ago

Selected Answer: C

C. Export device state. Checked in a lab
upvoted 3 times

Bulkozore 3 years, 5 months ago

Device state file is including both local and panorama configuration. C is not the right answers. I would say B.
upvoted 3 times

GivemeMoney 2 years, 7 months ago

Wrong, it's C do more research Bulkozore.
upvoted 3 times

bmarks 3 years, 6 months ago

Answer = C Export device state
"there is no "Export Device State" option available on the WebGUI of the Panorama"
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClgKCAS>
upvoted 5 times

TCoder 4 years, 1 month ago

Correct Answer
upvoted 6 times

Which two settings can be configured only locally on the firewall and not pushed from a Panorama template or template stack? (Choose two.)

- A. HA1 IP Address
- B. Master Key
- C. Zone Protection Profile
- D. Network Interface Type

Correct Answer: AB

  **ChiaPet75** Highly Voted 4 years, 2 months ago

Correct: A,B

You can use Templates and Template Stacks to define a wide array of settings but you can perform the following tasks only locally on each managed firewall:

Configure a device block list.

Clear logs.

Enable operational modes such as normal mode, multi-vsyst mode, or FIPS-CC mode.



Configure the IP addresses of firewalls in an HA pair.

Configure a master key and diagnostics.

Compare configuration files (Config Audit).

Renaming a vsyst on a multi-vsyst firewall.

upvoted 15 times

  **Raikin** 3 years, 4 months ago

It is possible to set up in Panorama, also for a secondary box via variables, but for some reason firewalls just don't take those values. Have PAN TAC case opened for it for 4 months already, PA engineering is working on it as of 04/2021. just fyi

upvoted 1 times

  **secdaddy** 1 year, 10 months ago

reference URL

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/template-capabilities-and-exceptions>

upvoted 1 times

  **Frightened_Acrobat** 1 year, 6 months ago

'Allow Forwarding of Decrypted Content' under Device->Setup->Content-ID->Content-ID Settings also cannot be configured on a Panorama Template. Has to be configured locally on the firewall.

upvoted 1 times

  **eeez27** Highly Voted 2 years, 1 month ago

I am pretty sure the HA IP address can be pushed from HA variables settings.

upvoted 6 times

  **Gngogh** 1 year, 10 months ago

i have configured a pair of PA where all HA conf is pushed from Pano

upvoted 5 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: AB

Correct answer is A and B


upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: AB

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/template-capabilities-and-exceptions>

upvoted 2 times

  **dcamps** 3 years, 3 months ago



<https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/template-capabilities-and-exceptions.html#idf414a976-3abc-42c3-a21e-63bc5b94c638>

upvoted 2 times

  **yoginangpal** 3 years, 3 months ago

Badly worded question as you can push master key from Panorama to firewalls but not via template or Template stack it is via Panorama Managed Devices Summary select the firewall and pick Deploy Master Key from task bar at the bottom, so technically the answer AB is correct as you cannot push Master Key via Template or Template stack. You cannot create HA IP and push from Panorama.

upvoted 2 times

  **lildevil** 1 year, 11 months ago

I don't see how you can't push HA1 IP's I have a template stack that has a template called active that does just this, and a second template stack called passive that does the same thing (all my HA1's are 192.168.1.1/30 and 192.168.1.2/30 respectively for active and passive)

upvoted 2 times

  **Gngogh** 1 year, 10 months ago

you can also use the same template stack on both firewalls and change HA IPs with variables

upvoted 2 times

  **yoginangpal** 3 years, 3 months ago

Badly worded question as you can push master key from Panorama to firewalls but not via template or Template stack it is via Panorama > Managed Devices > Summary select the firewall and pick Deploy Master Key from task bar at the bottom, however you are not pushing this change via Template or Template stack so technically the answer is AB

upvoted 1 times

An administrator just submitted a newly found piece of spyware for WildFire analysis. The spyware passively monitors behavior without the user's knowledge.

What is the expected verdict from WildFire?

- A. Malware
- B. Grayware
- C. Phishing
- D. Spyware

Correct Answer: B

  **bartbernini** Highly Voted 2 years, 7 months ago

Selected Answer: D

D. Grayware.

Although this *is* an example of spyware, that is not one of the four possible WildFire verdicts. From Palo Alto, "Grayware typically includes adware, spyware, and Browser Helper Objects (BHOs)."

<https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/wildfire-concepts/verdicts.html>

upvoted 15 times

  **eyelasers1** 2 years, 6 months ago

Don't you mean B. Grayware?

upvoted 2 times

  **Chris71Mach1** 1 year, 7 months ago

THIS is the explanation we all need. Thank you.


upvoted 3 times

  **apiloran** Most Recent 1 month, 2 weeks ago

Selected Answer: B

B. Grayware

upvoted 1 times

  **apiloran** 1 month, 3 weeks ago

Selected Answer: B

Grayware

—The sample does not pose a direct security threat, but might display otherwise obtrusive behavior. Grayware typically includes adware, spyware, and Browser Helper Objects (BHOs).

upvoted 1 times

  **hcir** 2 months, 2 weeks ago

malware and spyware verdicts do not exist in wildfire: and it is not phishing, so the only left is grayware. Answer B



upvoted 1 times

  **weze1336** 3 months, 1 week ago

Selected Answer: B

answer B Grayware

upvoted 1 times

  **weze1336** 3 months, 1 week ago

Answer is GRAYWARE. The question is specifically asking for "VERDICT".

There is NO verdict called "SPYWARE". "Spyware" is included within the "Grayware" Verdict. See Below.

Benign Indicates that the entry received a WildFire analysis verdict of benign. Files categorized as benign are safe and do not exhibit malicious behavior.

Grayware Indicates that the entry received a WildFire analysis verdict of grayware. Files categorized as grayware do not pose a direct security threat but might display otherwise obtrusive behavior. Grayware can include adware, spyware, and Browser Helper Objects (BHOs).

Phishing Indicates that WildFire assigned a link and analysis verdict of phishing. A phishing verdict indicates that the site to which the link directs users displayed credential phishing activity.

Malicious Indicates that the entry received a WildFire analysis verdict of malicious. Samples categorized as malicious can pose a security threat. Malware can include viruses, C2

(command-and-control), worms, Trojans, Remote Access Tools (RATs), rootkits, and botnets. For samples that are identified as malware, the WildFire cloud generates and distributes a signature to prevent against future exposure.

upvoted 2 times

[-] 👤 **Od2fdfa** 3 months, 3 weeks ago

Selected Answer: B

Verdict categories are Benign, Grayware , Phishing, Malicious

<https://docs.paloaltonetworks.com/advanced-wildfire/administration/advanced-wildfire-overview/advanced-wildfire-concepts/verdicts>
upvoted 1 times

[-] 👤 **123XYZT** 3 months, 3 weeks ago

I meant B is correct
upvoted 1 times

[-] 👤 **123XYZT** 3 months, 3 weeks ago

D is correct, the possible verdicts from Palo Alto are Benign, Grayware, Phishing and Malicious.
upvoted 1 times

[-] 👤 **Loloshikovichev** 4 months, 1 week ago

Selected Answer: B

There is no "Spyware" verdict.
upvoted 1 times

[-] 👤 **Marshpillowz** 7 months, 1 week ago

Apologies correct answer is B
upvoted 1 times

[-] 👤 **Marshpillowz** 7 months, 1 week ago

Selected Answer: D

Answer is D
upvoted 1 times

[-] 👤 **Sammy3637** 8 months, 4 weeks ago

Selected Answer: B

Spyware is a type of Grayware
upvoted 1 times

[-] 👤 **gully300** 1 year, 7 months ago

Selected Answer: B

bartbernini Highly Voted 11 months, 2 weeks ago
<correction>B</correction> Grayware.

Although this *is* an example of spyware, that is not one of the four possible WildFire verdicts. From Palo Alto, "Grayware typically includes adware, spyware, and Browser Helper Objects (BHOs)."

<https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/wildfire-concepts/verdicts.html>
upvoted 3 times

[-] 👤 **awtsuritauna** 1 year, 9 months ago

Answer is B

Grayware

—The sample does not pose a direct security threat, but might display otherwise obtrusive behavior. Grayware typically includes adware, spyware, and Browser Helper Objects (BHOs).

upvoted 1 times

[-] 👤 **TAKUM1y** 1 year, 11 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/wildfire/10-0/wildfire-admin/wildfire-overview/wildfire-concepts/verdicts>
upvoted 3 times

[-] 👤 **UFanat** 2 years, 2 months ago

Selected Answer: B

Grayware—The sample does not pose a direct security threat, but might display otherwise obtrusive behavior. Grayware typically includes adware, spyware, and Browser Helper Objects (BHOs).

upvoted 2 times

When configuring the firewall for packet capture, what are the valid stage types?

- A. receive, management, transmit, and non-syn
- B. receive, management, transmit, and drop
- C. receive, firewall, send, and non-syn
- D. receive, firewall, transmit, and drop

Correct Answer: D

— **zadkiel** Highly Voted 4 years, 1 month ago

correct is D
upvoted 12 times

— **chief_odogwu** Highly Voted 3 years, 7 months ago

Correct answer is D
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CITJCA0>
upvoted 8 times

— **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: D

D is correct
upvoted 1 times

— **TAKUM1y** 1 year, 11 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/monitor/monitor-packet-capture/packet-capture-overview>
upvoted 2 times

— **bartbernini** 2 years, 7 months ago

D is the correct answer. From Palo Alto, "You define the file name based on the stage (Drop, Firewall, Receive, or Transmit)." At first glance, you may select B, but to perform a packet capture of management traffic you would need to use tcpdump.

[://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/monitor/monitor-packet-capture/packet-capture-overview.html](https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/monitor/monitor-packet-capture/packet-capture-overview.html)
upvoted 3 times

— **ninjawrz** 2 years, 8 months ago

correct answer D
RX,TX,FW,DR
upvoted 5 times

Which operation will impact the performance of the management plane?

- A. DoS protection
- B. WildFire submissions
- C. generating a SaaS Application report
- D. decrypting SSL sessions

Correct Answer: C

— **smasyed** Highly Voted 4 years, 3 months ago

For Answer C: Both explaining "logging and reporting" are once causing MP high usage
TIPS & TRICKS: REDUCING MANAGEMENT PLANE LOAD:
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CISvCAK>

TIPS & TRICKS: REDUCING MANAGEMENT PLANE LOAD—PART 2:
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIU4CAK>
upvoted 17 times

— **HarryDang** Highly Voted 4 years, 3 months ago

C is correct
upvoted 9 times

— **Jared28** Most Recent 6 months, 1 week ago

Selected Answer: C

Reports are *ALWAYS* management plane, making C the best answer
For those saying D, in *some* configurations/firewalls the management plane may be used for SSL decryption.
upvoted 1 times

— **Marshpillowz** 7 months, 1 week ago

Selected Answer: C

C is correct
upvoted 1 times

— **ChiaPet75** 1 year ago

PCNSE Study Guide 2023 1.6
Every Palo Alto Networks firewall assigns a minimum of these functions to the management plane:

- Configuration management
- Logging
- Reporting functions <===
- User-ID agent process
- Route updates

upvoted 1 times

— **Merlin0o** 1 year, 2 months ago

Selected Answer: C

Correct is C

D is not correct as:

Identify the functions that reside on the data plane

The following functions are assigned to the data plane:

- Signature match processor • All Content-ID and App-ID services • Security processors • Session management
- Encryption and decryption <----- Data Plane, No impact on the MGMT plane.
- Compression and decompression
- Policy enforcement • Network processor • Route • Address Resolution Protocol (ARP) • MAC lookup • QoS • NAT • Flow control

Ref; Study guide page 50-51

upvoted 1 times

— **hpbdcB** 1 year, 11 months ago

Selected Answer: C

ssl decryption is done in hardware on higher models and on mgm for lower models, so for sure C will have an impact.
upvoted 2 times

— **Kuronekosama** 2 years ago

Selected Answer: D

SSL Decryption eats up CPU which directly impacts MGT. I'm going with D.


upvoted 1 times

  **redbull900** 2 years, 1 month ago

Selected Answer: D

SSL Decryption is done on the MGMT plane. <https://live.paloaltonetworks.com/t5/general-topics/where-is-ssl-processing-done-data-plane-or-management-plane/m-p/3722#M2739>



upvoted 1 times

  **kolz** 2 years, 9 months ago

Selected Answer: C



C is correct

upvoted 5 times

  **evdw** 3 years, 4 months ago

Correct Answer: C

upvoted 1 times

  **Qintao** 3 years, 4 months ago

B or C, not sure

upvoted 1 times

  **rocioha** 3 years, 5 months ago

C is the correct answer

upvoted 1 times

  **TamerRouby** 4 years, 3 months ago

Correct answer C

upvoted 4 times

Which User-ID method maps IP addresses to usernames for users connecting through a web proxy that has already authenticated the user?

- A. syslog listening
- B. server monitoring
- C. client probing
- D. port mapping

Correct Answer: A

  **aatechler** Highly Voted 1 year, 7 months ago

Selected Answer: A

Syslog:

The Windows-based User-ID agent and the PAN-OS integrated User-ID agent use Syslog Parse

Profiles to interpret login and logout event messages that are sent to syslog servers from devices that authenticate users. Such devices include wireless controllers, 802.1x devices, Apple Open Directory servers, proxy servers, and other network access control devices.

Server monitoring:

A Windows-based User-ID agent, or the built-in PAN-OS integrated User-ID agent inside the PAN-OS firewall, monitors Security Event logs for successful login and logout events on Microsoft domain controllers, Exchange servers, or Novell eDirectory servers.

upvoted 7 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: A

Answer is A

upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-id-to-monitor-syslog-senders-for-user-mapping/configure-the-pan-os-integrated-user-id-agent-as-a-syslog-listener#id91eb3abd-43c1-4969-8a5f-df032685e277>

upvoted 4 times

  **nekkrokvlt** 2 years ago

Correct answer should be <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/user-id-concepts/user-mapping/xff-headers>

upvoted 3 times

  **z8d21oczd** 2 years, 1 month ago

Selected Answer: B

Yes listen to syslogs. But this is configured in Server Monitoring Section were you create a new Server Monitor with type Syslog Sender. So, logically it is a syslog listener but in palo alto terms it is a server monitor

upvoted 4 times

  **z8d21oczd** 2 years, 1 month ago

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-id-to-monitor-syslog-senders-for-user-mapping/configure-the-pan-os-integrated-user-id-agent-as-a-syslog-listener#id91eb3abd-43c1-4969-8a5f-df032685e277>

upvoted 1 times

  **Gngogh** 1 year, 10 months ago


Server monitor can also be used to configure monitor for AD, Exchange and Novel-e. In this case Syslog listener is the most specific answer.

upvoted 1 times

  **venkat_narsimulu** 3 years, 4 months ago

Ans should be A

upvoted 4 times

  **nk12** 4 years ago

Correct Answer: A

To obtain user mappings from existing network services that authenticate users—such as wireless controllers, 802.1x devices, Apple Open Directory servers, proxy servers, or other Network Access Control (NAC) mechanisms—Configure User-ID to Monitor Syslog Senders for User Mapping.

upvoted 4 times

  **Chris71Mach1** 1 year, 7 months ago

Best/proper explanation for this. Thanks!

upvoted 1 times

  **petros_K** 4 years, 3 months ago

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/user-id-overview.html>
upvoted 1 times

  **rammsdoct** 4 years, 3 months ago

A:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/map-ip-addresses-to-users>
upvoted 2 times

Question #125

Topic 1

The firewall determines if a packet is the first packet of a new session or if a packet is part of an existing session using which kind of match?

- A. 6-tuple match: Source IP Address, Destination IP Address, Source Port, Destination Port, Protocol, and Source Security Zone
- B. 5-tuple match: Source IP Address, Destination IP Address, Source Port, Destination Port, Protocol
- C. 7-tuple match: Source IP Address, Destination IP Address, Source Port, Destination Port, Source User, URL Category, and Source Security Zone
- D. 9-tuple match: Source IP Address, Destination IP Address, Source Port, Destination Port, Source User, Source Security Zone, Destination Security Zone, Application, and URL Category

Correct Answer: A

  **MS_NW** Highly Voted 4 years, 1 month ago

A

On a Palo Alto Networks firewall, a session is defined by two uni-directional flows each uniquely identified by a 6-tuple key: source-address, destination-address, source-port, destination-port, protocol, and security-zone.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVECA0>

upvoted 15 times

  **PaloSteve** 1 year, 1 month ago

This is an AMAZING article to get to know a session in DETAIL.


upvoted 1 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times



  **certprep2021** 1 year, 7 months ago

Selected Answer: A

A



<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVECA0>

upvoted 2 times

  **Sarbi** 1 year, 8 months ago

It is always 5 tuples.

upvoted 1 times

  **mmed** 3 years, 5 months ago

confirm A

upvoted 3 times

Which GlobalProtect Client connect method requires the distribution and use of machine certificates?

- A. At-boot
- B. Pre-logon
- C. User-logon (Always on)
- D. On-demand

Correct Answer: B

rammsdoct Highly Voted 4 years, 3 months ago

for machine certificate it is B: Pre-Logon
if it was client certificate would be USER-LOGON

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIFoCAK>

go to part B on cert profile topic.
upvoted 9 times

MyWil 4 years ago

Rammsdoct you are correct based on the URL that you have provided: It says:
Client certificate refers to user cert, it can be used for 'user-logon'/'on-demand' connect methods. Used to authenticate a user.
-Machine certificate refers to device cert, it can be used for 'pre-logon' connect method. This is used to authenticate a device, not a user.
upvoted 3 times

Marshpillowz Most Recent 7 months, 1 week ago

Selected Answer: B

B is correct
upvoted 1 times

DenskyDen 1 year, 7 months ago

Selected Answer: B

Machine certificate refers to device cert, it can be used for 'pre-logon' connect method.
upvoted 1 times

TAKUM1y 1 year, 11 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-user-authentication/set-up-client-certificate-authentication/deploy-machine-certificates-for-authentication>
upvoted 2 times

TAKUM1y 1 year, 11 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-user-authentication/set-up-client-certificate-authentication>
upvoted 2 times

UFanat 2 years, 2 months ago

Selected Answer: B

B. Pre-logon requires machine cert
upvoted 2 times

Breyarg 2 years, 8 months ago

i have literally built this config too many times not to know the correct answer. 100% B and 100% the bane of my existence!
upvoted 1 times

Breyarg 2 years, 8 months ago

to elaborate, you also need to have the private key and the cert chain visible on the cert when installed on a host.
upvoted 1 times

Which feature can provide NGFWs with User-ID mapping information?

- A. Web Captcha
- B. Native 802.1q authentication
- C. GlobalProtect
- D. Native 802.1x authentication

Correct Answer: C

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: C

C is correct
upvoted 1 times

  **TAKUM1y** 1 year, 11 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/user-id-concepts/user-mapping>
upvoted 3 times

  **UFanat** 2 years, 2 months ago



Selected Answer: C

Only C :)
upvoted 2 times

  **confusion** 2 years, 5 months ago

Selected Answer: C



definitely C
upvoted 2 times

  **Gabuu** 2 years, 7 months ago

answer is C
upvoted 3 times

  **Narendragpt** 3 years, 6 months ago

its C ...
<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/user-id-concepts/user-mapping.html>
upvoted 4 times

  **qqqq123** 4 years ago

Yeah, FW populate UserID DBs from GlobalProtect. Then it can re-distribute it to other FWs
upvoted 4 times

  **DamiiE** 4 years ago

D Native 802.1x what do you guys think ?
upvoted 1 times

  **pollyy** 4 years ago

Correct answer is C
upvoted 4 times

Which Panorama administrator types require the configuration of at least one access domain? (Choose two.)

- A. Role Based
- B. Custom Panorama Admin
- C. Device Group
- D. Dynamic
- E. Template Admin

Correct Answer: CE

Ab121213 **Highly Voted** 4 years, 3 months ago

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIETCA0>

3.Create Administrator for Administrator Type "Device Group and Template Admin" and bind the access domain
upvoted 15 times

Pag0s **Highly Voted** 3 years, 6 months ago

C,E are correct I agree with Ab121213 provided link
upvoted 7 times

Marshpillowz **Most Recent** 7 months, 1 week ago

Selected Answer: CE

C and E correct
upvoted 1 times

JRKhan 7 months, 3 weeks ago

Selected Answer: CE

Access domains allow you to control which permissions a specific administrator has when that administrator accesses a set of managed devices through Panorama. Access domains use Device Group and Template permission sets that you must define beforehand.
upvoted 1 times

ccaiccie 8 months, 2 weeks ago

Answer is A, D
upvoted 1 times

djedeen 1 year, 7 months ago

Selected Answer: CE

Access domains apply only to administrators with Device Group and Template roles.
upvoted 1 times

TAKUM1y 1 year, 10 months ago

Selected Answer: CE

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/role-based-access-control/access-domains>
upvoted 2 times

qqqq123 4 years ago

Makes sense, access domain is some part of your installation. In Panorama there are two kinds of such parts - Templates(for device mgmt) and Device Groups(for traffic mgmt).
upvoted 4 times

Which option enables a Palo Alto Networks NGFW administrator to schedule Application and Threat updates while applying only new content-IDs to traffic?

- A. Select download-and-install
- B. Select download-only
- C. Select download-and-install, with "Disable new apps in content update" selected
- D. Select disable application updates and select "Install only Threat updates"

Correct Answer: C

  **Ab121213** Highly Voted 4 years, 3 months ago

Correct Answer C:

On the Device Dynamic Updates page, select Schedule . Choose to Disable new apps in content update for downloads and installations of content releases.



<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-releases/disable-or-enable-app-ids>

upvoted 19 times

  **sunjun** Highly Voted 4 years, 3 months ago

I think that c is correct

upvoted 7 times

  **rcn11** 4 years, 2 months ago



if I may ask, wouldn't that disable new content? in the question 'while applying only new content-IDs to traffic' - disabling new apps will keep the old app-id apps and won't have new content?

upvoted 5 times

  **zadkiel** 4 years, 1 month ago

Content-ID and App-ID is two different things. Content-ID is more related to threats, url filtering etc. App-ID is application visibility and control

upvoted 12 times

  **kraut** 3 years, 4 months ago

thanks for clarifying, I also got confused between the two!

upvoted 2 times

  **123XYZT** Most Recent 3 months, 3 weeks ago

The correct answer is A, since you want to start using the new content IDs, that's what's going to happen by default if you do download and install.

upvoted 1 times

  **327c7c8** 5 months, 1 week ago

the question is incorrectly formulated, I am really disappointed

It say "Applying only new Content-ID", in the update setting of the threat and application there are no mention of content-ID.

either you apply the new app-id or not.

As long as the question is requiring you to use/apply the newly content-ID why would you even consider disabling the new App-ID.

The question and the alternative is incorrect.

upvoted 1 times

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: C

C is correct



upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-releases/disable-or-enable-app-ids>

upvoted 2 times











  **KKQQ12345** 2 years ago

Selected Answer: C

App-ID <> Content-ID

"Disable new apps in content update" so only allow content updates without App-ID























upvoted 2 times

- [-]  **Pretorian** 2 years ago
What a malicious question man... (one of many)
upvoted 3 times
- [-]  **DriVen** 2 years, 1 month ago
Selected Answer: A
A is the correct answer!
C tells the opposite of what the question asks...
upvoted 2 times
- [-]  **UFanat** 2 years, 2 months ago
Selected Answer: C
C is correct.
upvoted 1 times
- [-]  **Didesh** 2 years, 5 months ago
Selected Answer: B
c says download-and-install.
question is asking about schedule Application and Threat updates while applying only new content-IDs to traffic""
B is correct in my opinion.
upvoted 1 times
- [-]  **tururu1496** 2 years, 6 months ago
Selected Answer: C
Answer: C
upvoted 1 times
- [-]  **yoginangpal** 3 years, 3 months ago
the correct answer is C you can apply new content ID but can disable the new apps in the content update, it is a checkbox this is prevent disruption due to new application ID installation
upvoted 2 times
- [-]  **evdw** 3 years, 4 months ago
Correct answer : C
upvoted 2 times
- [-]  **aadach** 3 years, 5 months ago
only C
upvoted 3 times
- [-]  **Pag0s** 3 years, 6 months ago
the question insisted on " while applying only new content-IDs to traffic"
the only acceptable ans is "A"
upvoted 3 times
- [-]  **bmarks** 3 years, 6 months ago
Answer = C
User Ab121213 provided the link that explains the answer to this question:
You can disable all App-IDs introduced in a content release if you want to immediately benefit from the latest threat prevention, and plan to enable the App-IDs later, and you can disable App-IDs for specific applications. Below is applicable link for PANOS 9.1
<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-releases/disable-or-enable-app-ids.html>
upvoted 3 times

Which is the maximum number of samples that can be submitted to WildFire per day, based on a WildFire subscription?

- A. 10,000
- B. 15,000
- C. 7,500
- D. 5,000

Correct Answer: A

-   **awtkas983** Highly Voted 4 years, 2 months ago
answer is 1000 however its not listed in the choices, I assume option A is a typo error it should be 1000 not 10,000..if it is, correct answer is A.
<https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/submit-files-for-wildfire-analysis/manually-upload-files-to-the-wildfire-portal.html#:~:text=All%20Palo%20Alto%20Networks%20customers,a%20day%20for%20WildFire%20analysis>
upvoted 11 times
-   **BTSeeYa** Most Recent 1 month, 2 weeks ago
They messed up the question. Clearly they meant automatic verdict queries, instead of submitted samples. That would be 10,000.
upvoted 1 times
-   **Marshpillowz** 7 months, 1 week ago
Selected Answer: A
Answer is 1000
upvoted 1 times
-   **Frightened_Acrobat** 1 year, 6 months ago
Actually... D is the only answer that fits. Total daily submissions for standard Wildfire is 150. There are two problems with including the query limits of 1050: a) $150 + 1050 \neq 1,000$. b) The question specifically asks for "submissions."
The only Wildfire limit that matches one of these numbers is D, 5,000. Prisma Cloud Compute limits daily Wildfire submissions to exactly 5,000.
<https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-api/about-the-wildfire-api/wildfire-api-access-control/impose-api-limits>
upvoted 3 times
-   **olori7170** 1 year, 10 months ago
The answer is 1000, As part of the WildFire subscription, you can submit up to 150 sample submissions and up to 1,050 sample queries a day.
upvoted 2 times
-   **Gngogh** 1 year, 10 months ago
This information has changed!!!
<https://docs.paloaltonetworks.com/wildfire/10-0/wildfire-admin/wildfire-overview/wildfire-subscription>
upvoted 1 times
-   **TAKUM1y** 1 year, 10 months ago
Selected Answer: A
<https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/wildfire-subscription>
From version 8.1 onwards [you can submit up to 150 sample submissions and up to 1,050 sample queries a day.]
upvoted 3 times
-   **GivemeMoney** 2 years, 7 months ago
<https://docs.paloaltonetworks.com/wildfire/10-1/wildfire-admin/wildfire-overview/wildfire-subscription.html> - "The WildFire API supports up to 1,000 file submissions and up to 10,000 queries a day."
upvoted 4 times
-   **ronin999** 2 years, 8 months ago
A. 10,000 submissions 1,000 API queries
upvoted 3 times
-   **YasserSaied** 3 years, 2 months ago
1000 per day --
upvoted 1 times
-   **qqqq123** 4 years ago
Yeah, seems like a mistake in answer options:
"The WildFire API supports up to 1,000 file submissions and up to 10,000 queries a day."
<https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/wildfire-overview/wildfire-subscription>
upvoted 4 times

In which two types of deployment is active/active HA configuration supported? (Choose two.)

- A. Layer 3 mode
- B. TAP mode
- C. Virtual Wire mode
- D. Layer 2 mode

Correct Answer: AC

  **MS_NW** Highly Voted 4 years, 1 month ago

A and C

Active/Active— Both firewalls in the pair are active and processing traffic and work synchronously to handle session setup and session ownership. Both firewalls individually maintain session tables and routing tables and synchronize to each other. Active/active HA is supported in virtual wire and Layer 3 deployments.

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/high-availability/ha-concepts/ha-modes>

upvoted 16 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: AC

A and C correct

upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: AC

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/ha-modes>

upvoted 3 times

  **Narendragpt** 3 years, 6 months ago

AC... <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/high-availability/ha-concepts/ha-modes#:~:text=Active%2Fpassive%20HA%20is%20supported,such%20as%20IPSec%20security%20associations.>

upvoted 3 times

For which two reasons would a firewall discard a packet as part of the packet flow sequence? (Choose two.)

- A. ingress processing errors
- B. rule match with action \neq deny \neq
- C. rule match with action \neq allow \neq
- D. equal-cost multipath

Correct Answer: AB

  **Daniel2020** Highly Voted  3 years, 10 months ago

A and B

Denying traffic will discard the packet. Packets can also be discarded due to malformed or incorrect frames, datagrams or packets.

C and D are irrelevant as packets would never be discarded if allowed and ECMP simply allows the use of multiple routes or paths to a destination.

Read up on "Packer Flow Sequence", it details where exactly it will discard packets (layer 2, layer 3 and on)

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVHCA0>

upvoted 13 times

  **Marshpillowz** Most Recent  7 months, 1 week ago

Selected Answer: AB

A and B correct

upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: AB

A and B only suitable answers

upvoted 2 times

  **Prutser2** 3 years, 2 months ago

common sense question a and b

upvoted 4 times

Which logs enable a firewall administrator to determine whether a session was decrypted?

- A. Traffic
- B. Security Policy
- C. Decryption
- D. Correlated Event

Correct Answer: A

  **Daniel2020** Highly Voted 3 years, 7 months ago

A is the answer and not C.

Yes in PAN-OS 10 the Decryption Log was introduced but that is more suited for troubleshooting where decryption broke the SSL/TLS session. It is far easier to check if a session was decrypted by checking the Traffic Log.



It is clear here in the PAN-OS 10 Admin guide, section "Verify Decryption", that to check the Traffic Log to verify if decryption happened. Silly enough it also states in the very same document that you can check the decryption log (but, it seems to miss out that only for decryption failures). <https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/verify-decryption.html>

Here is the link for Decryption Log, you will read that it only logs unsuccessful decryption attempts. <https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/troubleshoot-and-monitor-decryption/decryption-logs.html#idb1b7e4a6-b48c-4ca7-8569-b785da780dd6>

Now I am not running PAN-OS 10 in the real world so I can't say 100% but reading off the documentation, that is how I would answer the question.
upvoted 11 times

  **CyberG** Highly Voted 3 years, 6 months ago

As of, August 17th, the Palo Alto Networks Certified Network Security Engineer (PCNSE) and the Palo Alto Networks Certified Network Security Administrator (PCNSA) certification exams reflect changes based on PAN-OS 10.0. Correct Answer is C
<https://live.paloaltonetworks.com/t5/certification-articles/pcnse-and-pcnsa-exam-changes-with-10-0/ta-p/344832>
upvoted 8 times

  **GohanF2** 1 year, 6 months ago

This is true. Answer is C. The new exam is evaluating version. 10.0
upvoted 1 times

  **duckduckgoo** 1 year, 5 months ago

A
You missed the key word, whether or not it was decrypted. Decryption log is used for troubleshooting if decryption was busted, NOT whether or not something was decrypted.
upvoted 2 times



  **BTSeeYa** Most Recent 1 month, 2 weeks ago

Old question, probably before there even were Decryption logs. I'd still put Traffic though, just because you can filter by Decrypted column really easy.
upvoted 1 times

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: A

A is correct
upvoted 1 times

  **javim** 1 year, 7 months ago


Selected Answer: A

I think A, because it say "whether a session was decrypted". Decryption log is for traffic is already decrypted, but in Traffic log you can see if the traffic is decrypted or not.
upvoted 2 times

  **dogeatdog** 1 year, 8 months ago

Selected Answer: C



C not A on 10.2 and 11.0
upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/verify-decryption>

upvoted 4 times

  **spydog** 1 year, 11 months ago

Selected Answer: A

Although the newer version have dedicate log type for "Decryption", as others already pointed out, those logs can be used to troubleshoot decryption/negotiations issues. The question is asking how you can determine if session was decrypted - the best way to is still to check the details of the traffic log and see if the flag "decrypted" is checked.

In addition, according to documentations by default only the unsuccessful decryption handshakes will be logged under "Decryption", which means if session is successfully decrypted, no log will be shown here and you might think that session was not decrypted.

upvoted 3 times

  **dien1991** 2 years, 4 months ago

Selected Answer: A

Traffic log can show status of decryption or not first.

upvoted 3 times

  **Jared28** 2 years, 5 months ago

Selected Answer: A

If a security rule is logging it will always show if it was decrypted (and is the simplest thing to look at). By default, the decryption rules log only on unsuccessful SSL handshakes. If you're troubleshooting, this is the log to go look at but if all you want to do is figure out decrypted yes/no, traffic log even in 10.0+.

upvoted 1 times

  **GivemeMoney** 2 years, 7 months ago

Selected Answer: C


There is now a decryption log: <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/troubleshoot-and-monitor-decryption/decryption-logs.html>

upvoted 1 times

  **GivemeMoney** 2 years, 7 months ago

Per reading the document Monitor>Logs>Traffic traffic logs seems to be right after all, i change to answer A.

upvoted 1 times

  **Joey456** 3 years, 3 months ago

A is correct: Decryption logs are dependent on traffic logs being enabled.

PAN-OS 10 doc cited here:

The Decryption log learns each session's App-ID from the Traffic log, so Traffic logs must be enabled to see the App-ID in the Decryption log. If Traffic logs are disabled, the App-ID shows as incomplete.

upvoted 2 times

  **frodo1791** 3 years, 4 months ago

The exam is based in panos 9.1 as far as I know, so answer should be A.

upvoted 1 times

  **bmarks** 3 years, 6 months ago

Please keep in mind, the PCNSE 9 exam focuses only on PANOS 9.1

Answer = A

Question is simply asking which log shows whether a session was decrypted.

upvoted 2 times

  **PAUGURU** 3 years, 8 months ago

Palo Alto introduces questions on the new version when it gets to the X.1.



So since now it is 10.0 the exam focuses on the 9.1 version, so correct answer is A, for the time being.

upvoted 4 times

  **MS_NW** 3 years, 9 months ago



Answer is A. There's no thing as Decryption log.

upvoted 1 times

  **Ali526** 3 years, 8 months ago

Correct, but starting Version 10, there IS a 'decryption log'. PA should fix this question.

upvoted 2 times

  **ricky69** 3 years, 9 months ago

Ans is C

The Decryption Log (Monitor

Logs

Decryption

) provides comprehensive information about sessions that match a Decryption policy to help you gain context about that traffic so you can accurately and easily diagnose and resolve decryption issues. The firewall does not log traffic if the traffic does not match a Decryption policy.

upvoted 2 times

  **brah_brah** 3 years, 10 months ago

v10 answer is C

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/troubleshoot-and-monitor-decryption/decryption-logs.html>
upvoted 4 times

An administrator needs to upgrade an NGFW to the most current version of PAN-OS® software. The following is occurring:

- ☞ Firewall has internet connectivity through e 1/1.
- ☞ Default security rules and security rules allowing all SSL and web-browsing traffic to and from any zone.
- ☞ Service route is configured, sourcing update traffic from e1/1.
- ☞ A communication error appears in the System logs when updates are performed.
- ☞ Download does not complete.

What must be configured to enable the firewall to download the current version of PAN-OS software?

- A. Static route pointing application PaloAlto-updates to the update servers
- B. Security policy rule allowing PaloAlto-updates as the application
- C. Scheduler for timed downloads of PAN-OS software
- D. DNS settings for the firewall to use for resolution

Correct Answer: D

rammsdoct Highly Voted 4 years, 3 months ago

D:

A cant be, there is no static service route to point to "palo alto updates" question is regarding that there is existing internet connection, so, default route should exist,

B: security policy allowing SSL traffic already exist so there is access from any to any

C: there is no scheduler involved on errors recurring with communication,

D: is the most closer to the issue, so D is correct.

upvoted 27 times

Woody 1 year, 8 months ago

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-upgrade/upgrade-pan-os/pan-os-upgrade-checklist#id53a2bc2b-f86e-4ee5-93d7-b06aff837a00>

upvoted 1 times

cerifyme85 6 months, 2 weeks ago

The main reason it is not be is that Updates happen through mgmt palne.. mgmt plane does not use security policies

upvoted 1 times

tobaja 3 months, 3 weeks ago

The question literally describes a service route, so it goes through the data plane.

upvoted 1 times

CiscoNinja Highly Voted 4 years, 3 months ago

The Default security rules and security rules allowing all SSL and web-browsing traffic to and from any zone. covers that (B is wrong) correct ans =

D

upvoted 11 times

apiloran Most Recent 1 month, 3 weeks ago

Selected Answer: D

The key word is default rule.

upvoted 1 times

weze1336 3 months, 1 week ago

Selected Answer: D

D

It's NOT B because the security rules already exist any to any zone for SSL

upvoted 1 times

123XYZT 3 months, 3 weeks ago

D is correct

upvoted 1 times

scanossa 6 months, 1 week ago

Selected Answer: D

It is between B or D:

B. Interface is facing the Internet directly, so it would be intranet (allowed by default)

D. It is needed to be configured in order to translate PA URL into IP addresses

So, D is correct

upvoted 1 times

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: D

Answer is D



upvoted 1 times

  **TeachTrooper** 7 months, 2 weeks ago

Selected Answer: D

B is wrong because of the default ruleset being in use, so the intrazone rule allows paloalto-updates app. D is correct as "generic communication error" on updates is usually a DNS issue

upvoted 1 times

  **JRKhan** 7 months, 3 weeks ago

Selected Answer: D

Given that question mentions about the communication error, D is the most appropriate answer. If the policy was denying it, the logs will mention traffic dropped/denied due to a configured policy rule or lack of a policy rule.

upvoted 1 times

  **DatITGuyTho1337** 8 months, 2 weeks ago

I believe D is the answer because the updates must be downloaded from the "updates.paloaltonetworks.com" site, the firewall must have DNS configured to take advantage of this. As DNS configuration was not mentioned during the question preface, I concluded that DNS must not have been configured.

upvoted 1 times

  **electro165** 1 year ago

Selected Answer: D

DNS Resolution: When the firewall attempts to download updates or software, it needs to resolve domain names to IP addresses to reach the update servers. If there's an issue with DNS resolution, it can lead to communication errors and incomplete downloads.

The other options (A, B, and C) do not directly address the issue of DNS resolution. While static routes, security policies, and scheduled downloads may be important for overall firewall configuration, they are not the primary factor for resolving domain names to IP addresses during the update process.

upvoted 1 times

  **Betty2022** 1 year, 1 month ago

Selected Answer: D



D, as per discussion shared by others here.

B: is covered, so this is not the answer because SSL and Web browsing is allowed.

Also, <https://applipedia.paloaltonetworks.com/> confirms that paloalto-updates would not give us any more access because : Implicit use

Applications: ssl, web-browsing

upvoted 1 times

  **sov4** 1 year, 1 month ago

Had this question a few weeks ago on the exam... July 2023. I'm going with D.



upvoted 1 times

  **ARWANGSH** 1 year, 2 months ago

Selected Answer: B



Palo Alto requires their update APPIDs to be allowed, this is not mentioned in the question.

upvoted 2 times

  **hz78** 1 year, 2 months ago

The communication error and incomplete download of updates suggest that the firewall is unable to resolve the update server's hostname to its IP address. To resolve this issue, the firewall needs proper DNS settings configured. By providing DNS settings, the firewall will be able to perform hostname resolution and establish connectivity with the update servers to download the PAN-OS software.

upvoted 2 times

  **p48m1** 1 year, 5 months ago

Selected Answer: B

B is correct.

Palo alto updates are recognized with App-ID "paloalto-updates", which makes implicit use of ssl and web-browsing. Creating a Security Policy with the proper App-ID will solve the download issue.

It is not a DNS issue, as "the download does not complete" implies a communication to be in place (then blocked due to App-ID mismatch) and proper name resolution to be successful.

upvoted 5 times

  **kewokil120** 1 year, 5 months ago

Selected Answer: B

Not dns. If it started then Dns worked. Palo does have 10+ app id for their saas upgrades etc
upvoted 1 times

Question #135

Topic 1

A client has a sensitive application server in their data center and is particularly concerned about session flooding because of denial-of-service attacks.

How can the Palo Alto Networks NGFW be configured to specifically protect this server against session floods originating from a single IP address?

- A. Add an Anti-Spyware Profile to block attacking IP address
- B. Define a custom App-ID to ensure that only legitimate application traffic reaches the server
- C. Add QoS Profiles to throttle incoming requests
- D. Add a tuned DoS Protection Profile

Correct Answer: D

  **nicolasjiang** **Highly Voted**  4 years, 1 month ago

correct D
upvoted 8 times

  **Marshpillowz** **Most Recent**  7 months, 1 week ago

Selected Answer: D

D is correct
upvoted 1 times



  **omgt2k2** 8 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules#:~:text=DoS%20Protection%20policy%20rules%20determine,help%20defend%20against%20DoS%20attacks.>
upvoted 1 times

  **Prutser2** 3 years, 2 months ago

answr d
upvoted 3 times

  **Woody** 1 year, 8 months ago

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules/dos-protection-profiles>
upvoted 2 times

  **mattass** 4 years, 3 months ago

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CImTCAS>
upvoted 4 times

An administrator deploys PA-500 NGFWs as an active/passive high availability pair. The devices are not participating in dynamic routing, and preemption is disabled.

What must be verified to upgrade the firewalls to the most recent version of PAN-OS® software?

- A. Antivirus update package.
- B. Applications and Threats update package.
- C. User-ID agent.
- D. WildFire update package.

Correct Answer: B

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/upgrade-to-pan-os-80/upgrade-the-firewall-to-pan-os-80/upgrade-an-ha-firewall-pair-to-pan-os-80>



  **bloodtech** Highly Voted 3 years, 5 months ago

Should be B
upvoted 6 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: B

B is correct
upvoted 1 times

  **lol12** 1 year, 10 months ago



Selected Answer: B

B
<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/upgrade-pan-os/upgrade-the-firewall-pan-os/upgrade-an-ha-firewall-pair-to-pan-os-10-2>
upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: B

Before upgrade you should check App and Threat update package version or update it to the latest one
upvoted 3 times

  **Gabuu** 2 years, 7 months ago

B
<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/upgrade-to-pan-os-90/upgrade-the-firewall-to-pan-os-90/upgrade-an-ha-firewall-pair-to-pan-os-90.html#idab14f5f2-f662-4e5c-ba5b-2cc35993e2ec>

step 3. number 1
upvoted 4 times

A firewall administrator has been asked to configure a Palo Alto Networks NGFW to prevent against compromised hosts trying to phone-home or beacon out to external command-and-control (C2) servers.
Which Security Profile type will prevent these behaviors?

- A. Anti-Spyware
- B. WildFire
- C. Vulnerability Protection
- D. Antivirus

Correct Answer: A

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/anti-spyware-profiles>

  **MyWil** Highly Voted 4 years, 1 month ago

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/anti-spyware-profiles>

Anti-Spyware profiles blocks spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers, allowing you to detect malicious traffic leaving the network from infected clients. You can apply various levels of protection between zones. For example, you may want to have custom Anti-Spyware profiles that minimize inspection between trusted zones, while maximizing inspection on traffic received from an untrusted zone, such as internet-facing zones.

A is Correct

upvoted 14 times

  **mmed** Highly Voted 3 years, 5 months ago

Anti-spyware

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles>

upvoted 6 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

  **ChiaPet75** 1 year ago

Best Practices Security Profiles

Attach an Anti-Spyware profile to all allowed traffic to detect command-and-control traffic (C2) initiated from malicious code running on a server or endpoint and prevent compromised systems from establishing an outbound connection from your network.

https://docs.paloaltonetworks.com/best-practices/internet-gateway-best-practices/best-practice-internet-gateway-security-policy/create-best-practice-security-profiles#ide042a854-cf6c-4535-a54b-6def3b2350ed_id17A29C0201H::~:~:text=may%20carry%20threats.,Best%20Practice%20Internet%20Gateway%20Antivirus%20Profile,-Clone%20the%20default

Clone%20the%20default

upvoted 1 times

  **awtsuritauna** 1 year, 9 months ago

Option A

<https://docs.paloaltonetworks.com/network-security/security-policy/security-profiles/security-profile-anti-spyware>

upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/security-profiles>

upvoted 3 times

What should an administrator consider when planning to revert Panorama to a pre-PAN-OS 8.1 version?

- A. Panorama cannot be reverted to an earlier PAN-OS release if variables are used in templates or template stacks.
- B. An administrator must use the Expedition tool to adapt the configuration to the pre-PAN-OS 8.1 state.
- C. When Panorama is reverted to an earlier PAN-OS release, variables used in templates or template stacks will be removed automatically.
- D. Administrators need to manually update variable characters to those used in pre-PAN-OS 8.1.

Correct Answer: A

Reference:

<https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/upgrade-to-pan-os-81/upgradedowngrade-considerations>

  **ars110** Highly Voted 4 years ago

A is correct

You are unable to downgrade from PAN-OS 8.1 to an earlier PAN-OS release if variables are used in your template or template stack configuration. Variables must be removed from the template and template stack configuration to downgrade.

upvoted 9 times

  **ChiaPet75** 1 year ago

It took me a while to actually find a PANOS release note from 8.1.

https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/8-1/pan-os-new-features/pan-os-new-features.pdf

upvoted 1 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times




Which two methods can be configured to validate the revocation status of a certificate? (Choose two.)

- A. CRL
- B. CRT
- C. OCSP
- D. Cert-Validation-Profile
- E. SSL/TLS Service Profile

Correct Answer: AC

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/certificate-management/set-up-verification-for-certificate-revocation-status>

  **mattass** Highly Voted  4 years, 3 months ago

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/certificate-management/certificate-revocation.html#idaa3aa4f6-4791-4dbb-b834-58c22e208be8>

upvoted 7 times

  **rammsdoct** 4 years, 2 months ago

yes A-C are correct

upvoted 10 times

  **Marshpillowz** Most Recent  7 months, 1 week ago

Selected Answer: AC

A and C correct



upvoted 1 times

  **aatechler** 1 year, 7 months ago

Selected Answer: AC

To verify the revocation status of certificates, the firewall uses Online Certificate Status Protocol (OCSP) and/or certificate revocation lists (CRLs).


upvoted 2 times

  **lol12** 1 year, 10 months ago

Selected Answer: AC

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/set-up-verification-for-certificate-revocation-status>

upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: AC

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/certificate-revocation>

upvoted 3 times

Which administrative authentication method supports authorization by an external service?

- A. Certificates
- B. LDAP
- C. RADIUS
- D. SSH keys

Correct Answer: C

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/firewall-administration/manage-firewall-administrators/administrative-authentication>

  **Mr_Cipher** Highly Voted  3 years, 8 months ago

C is a correct ans
upvoted 8 times



  **dwreck** Most Recent  3 months ago

Note "authorization" vs "authentication"... tricky tricky
upvoted 1 times



  **Marshpillowz** 7 months, 1 week ago

Selected Answer: C

C is correct
upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

Definitely C.
upvoted 1 times

  **Woody** 1 year, 8 months ago

B or and C
upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication>
upvoted 2 times

  **msevis** 4 years ago

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication>
upvoted 3 times

Which three file types can be forwarded to WildFire for analysis as a part of the basic WildFire service? (Choose three.)

- A. .dll
- B. .exe
- C. .fon
- D. .apk
- E. .pdf
- F. .jar

Correct Answer: ABC

Mello Highly Voted 5 years, 3 months ago

As part of the basic subscription, wildwire only submits PE files. This would include .exe .dll .fon and .src
upvoted 32 times

Levis 4 years ago

its not .src, it should be .scr
otherwise correct
upvoted 7 times

Gabriel2022 2 years ago

ADVANCED

WildFire Advanced File Type Support

—In addition to PEs, forward advanced file types for WildFire analysis, including APKs, Flash files, PDFs, Microsoft Office files, Java Applets, Java files (.jar and .class), and HTTP/HTTPS email links contained in SMTP and POP3 email messages. (WildFire private cloud analysis does not support APK, Mac OS X, Linux (ELF), archive (RAR/7-Zip), and script (JS, BAT, VBS, Shell Script, PS1, and HTA) files).

upvoted 1 times

Edu147 Highly Voted 5 years, 1 month ago

Correct answers A, B, C.

<https://docs.paloaltonetworks.com/wildfire/8-0/wildfire-admin/wildfire-overview/wildfire-subscription#>

First lines are the basic files supported, and middle lines the files supported with a paid subscription

upvoted 11 times

john_bosco_champion 4 years, 2 months ago

Sorry... You are correct... There's a Basic and Advanced subscription. The advanced one is what allows D,E,F.

upvoted 2 times

john_bosco_champion 4 years, 2 months ago

You are wrong. Answer is D,E,F

<https://docs.paloaltonetworks.com/wildfire/8-0/wildfire-admin/wildfire-overview/wildfire-file-type-support.html>

upvoted 2 times

shinichi_88 2 years, 7 months ago

A B C are correct, as stated "The basic WildFire service is included as part of the Palo Alto Networks next generation firewall and does not require a WildFire subscription. With the basic WildFire service, the firewall can forward portable executable (PE) files for WildFire analysis"

upvoted 1 times

123XYZT Most Recent 3 months, 3 weeks ago

A B C

Palo Alto Networks firewalls with a WildFire license are entitled to the standard subscription features and additional features. More file types may be submitted by a firewall for analysis. Additional file types are Microsoft Office files, PDF files, Java JAR and CLASS files, Adobe Flash SWF and SWC files, RAR, 7-Zip, Linux ELF, and Android APK files. The macOS Mach-O, DMG, and PKG files also are supported. WildFire also can analyze JS, VBS, and PS1 files.

upvoted 1 times

Marshpillowz 7 months, 1 week ago

Selected Answer: ABC

A, B and C correct

upvoted 1 times

Grace_Shu 1 year ago

Portable Executable
Filename extension

.acm, .ax, .cpl, .dll, .drv, .efi, .exe, .mui, .ocx, .scr, .sys, .tsp

upvoted 1 times

  **Redrum702** 1 year, 2 months ago

DEF:

Android application package apk, ETC.
Adobe Flash .swf, ETC.
Java Archive jar, ETC.
Microsoft Office docx, xlsx, pptx, ooxml, ETC.
Portable executable pe, exe, ETC.
Portable Document Format pdf, ETC.
Mac OS X dmg, pkg, ETC.
Archive rar, 7z, ETC.
Linux elf, ETC.
Script bat, js, vbs, ps1, ETC.

upvoted 2 times

  **Waheeladawy** 1 year, 4 months ago

Selected Answer: ABC

Answer will be A & B & C

Beacuse the Question ask for " basic WildFire service " find PaloAlto Docs talk about PAN WildFire Subscription

<https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/wildfire-subscription#idb6afc7db-1bcf-43e8-bdd3-7affa9aadda>

it mention the basic WildFire service, the firewall can forward portable executable (PE) files for WildFire, and see Below Docs

<https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/wildfire-concepts/file-analysis>

says that PEs Filetype include executable files, object code, DLLs, FON (fonts), and LNK files so A & B & C will be correct

upvoted 1 times

  **a_kto_to** 1 year, 4 months ago

According to WildFire documentation, the correct answer is: D, E, F

<https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/wildfire-concepts/file-analysis>

upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

Selected Answer: ABC

PEs include executable files, object code, DLLs, FON (fonts), and LNK files

upvoted 2 times

  **Pretorian** 2 years ago

Wow these answers are REALLY/totally wrong LOL

upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: ABC



<https://docs.paloaltonetworks.com/wildfire/10-1/wildfire-admin/wildfire-overview/wildfire-subscription>

The basic WildFire service is included as part of the Palo Alto Networks next generation firewall and does not require a WildFire subscription. With the basic WildFire service, the firewall can forward portable executable (PE) files for WildFire analysis

<https://docs.paloaltonetworks.com/wildfire/10-1/wildfire-admin/wildfire-overview/wildfire-concepts/file-analysis>

PEs include executable files, object code, DLLs, FON (fonts), and LNK files

upvoted 1 times

  **Jheax** 2 years, 4 months ago

Selected Answer: ABC

PDF, JAR, and APK are part of the advanced Wildfire license. So those cannot be the answer, leaving only A, B, and C.

upvoted 2 times

  **ramasamymuthiah** 2 years, 4 months ago

A, B, and C is the correct answer.


upvoted 1 times

  **Abu_Muhammad** 2 years, 5 months ago

Selected Answer: ABC

with basic subscription, only PE can be sent. A, B & C



upvoted 2 times

  **Bryan1151** 2 years, 8 months ago

From Beacon:

The standard service enables firewalls to automatically submit unknown Windows Portable Executable (or PE) files for analysis. Windows PE file types include EXE, DLL, SCR, and FON.

upvoted 1 times

  **FS68** 2 years, 10 months ago

A,B,C for basic subscription

upvoted 2 times

  **joaohbert** 2 years, 11 months ago

D,E and F are correct! WildFire Advanced File Type Support—In addition to PEs, forward advanced file types for WildFire analysis, including APKs, Flash files, PDFs, Microsoft Office files, Java Applets, Java files (.jar and .class), and HTTP/HTTPS email links contained in SMTP and POP3 email messages. (WildFire private cloud analysis does not support APK, Mac OS X, Linux (ELF), archive (RAR/7-Zip), and script (JS, BAT, VBS, Shell Script, PS1, and HTA) files). <https://docs.paloaltonetworks.com/wildfire/8-1/wildfire-admin/wildfire-overview/wildfire-subscription.html>

upvoted 1 times

An administrator has been asked to configure active/active HA for a pair of firewalls. The firewalls use Layer 3 interfaces to send traffic to a single gateway IP for the pair.

Which configuration will enable this HA scenario?

- A. The two firewalls will share a single floating IP and will use gratuitous ARP to share the floating IP.
- B. Each firewall will have a separate floating IP, and priority will determine which firewall has the primary IP.
- C. The firewalls do not use floating IPs in active/active HA.
- D. The firewalls will share the same interface IP address, and device 1 will use the floating IP if device 0 fails.

Correct Answer: A

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/floating-ip-address-and-virtual-mac-address>

  **eyelasers1** Highly Voted 2 years, 6 months ago

ANSWER: A

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/high-availability/ha-concepts/floating-ip-address-and-virtual-mac-address.html>

"each HA firewall interface has its own IP address and floating IP address. The interface IP address remains local to the firewall, but the floating IP address moves between the firewalls upon firewall failure.

If a link or firewall fails or a path monitoring event causes a failover, the floating IP address and virtual MAC address move over to the functional firewall. ... The functioning firewall sends a gratuitous ARP to update the MAC tables of the connected switches to inform them of the change in floating IP address

upvoted 7 times

  **TAKUM1y** Highly Voted 1 year, 10 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/floating-ip-address-and-virtual-mac-address>

upvoted 5 times

  **apiloran** Most Recent 1 month, 2 weeks ago

Selected Answer: A

ANSWER: A

The Key word is single gateway.

upvoted 1 times

  **ATRRHMN** 1 month, 4 weeks ago

Selected Answer: B

https://docs.paloaltonetworks.com/content/techdocs/en_US/pan-os/11-0/pan-os-admin/high-availability/ha-concepts/floating-ip-address-and-virtual-mac-address.html

https://docs.paloaltonetworks.com/content/techdocs/en_US/pan-os/11-0/pan-os-admin/high-availability/set-up-activeactive-ha/determine-your-activeactive-use-case/use-case-configure-activeactive-ha-with-floating-ip-addresses.html

upvoted 1 times

  **evilCorpBot7494** 5 months, 1 week ago

Selected Answer: B

Each firewall has its own floating IP. The fact they both send information to a same gateway doesn't mean they need to have just one floating IP, and the use case Palo Alto pushes is 1 floating IP for each Firewall, that can at any moment go to the other firewall in case the original owner of one of them fails.

Study Guide Page 180 and <https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/high-availability/set-up-activeactive-ha/determine-your-activeactive-use-case/use-case-configure-activeactive-ha-with-floating-ip-addresses>

upvoted 2 times

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

  **Xuzi** 9 months, 3 weeks ago

Selected Answer: A

The active/active HA firewalls share a single floating IP address that you bind to whichever firewall is in the active-primary state. With only one floating IP address, network traffic flows predominantly to a single firewall, so this active/active deployment functions like an active/passive deployment.

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/set-up-activeactive-ha/determine-your-activeactive-use-case/use-case-configure-activeactive-ha-with-floating-ip-address-bound-to-active-primary-firewall#id93973f10-2001-4ae4-b475-faa7e70967c1>
upvoted 1 times

  **gc999** 10 months, 1 week ago

Selected Answer: B

I will choose B. "Each HA firewall interface has its own IP address and floating IP address. The interface IP address remains local to the firewall, but the floating IP address moves between the firewalls upon firewall failure". That means each firewall has its own floating IP

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/ha-concepts/floating-ip-address-and-virtual-mac-address#:~:text=each%20HA%20firewall%20interface%20has%20its%20own%20IP%20address%20and%20floating%20IP%20address>
upvoted 1 times

  **Spaz_6** 1 year, 5 months ago



Selected Answer: A

answer is A. I got this in practice pcnse
upvoted 1 times

  **daytonadave2011** 1 year, 5 months ago

Selected Answer: A

A is the correct answer. This question is on Palo Alto Beacon.
upvoted 1 times

  **Gab99** 1 year, 6 months ago

Selected Answer: A

It depends,


1. With L3 Szenario with Active/Active deployment that behaves like Active/Passive deployment (Use Case: Configure Active/Active HA with Floating IP Address Bound to Active-Primary Firewall, <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/set-up-activeactive-ha/determine-your-activeactive-use-case#id726797f4-7d7b-4204-b86c-42589d19e8ac>) there is only ONE FLOATING IP.

2. There is also a use case with TWO FLOATING IPs, so please be careful with your assumptions.

From the description I would say "Standard L3 use case" (with active/active for faster failover), so only ONE FLOATING IP. >>> ANSWER A



But maybe the use case is the other, not 100% sure.

upvoted 2 times

  **DenskyDen** 1 year, 7 months ago

B. each HA firewall interface has its own IP address and floating IP address. The interface IP address remains local to the firewall, but the floating IP address moves between the firewalls upon firewall failure.

upvoted 2 times

  **mohr22** 1 year, 7 months ago

A

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/ha-concepts/arp-load-sharing>

upvoted 1 times

  **mohr22** 1 year, 6 months ago

In such a scenario, all hosts are configured with a single gateway IP address. One of the firewalls responds to ARP requests for the gateway IP address with its virtual MAC address. Each firewall has a unique virtual MAC address generated for the shared IP address. The load-sharing algorithm that controls which firewall will respond to the ARP request is configurable; it is determined by computing the hash or modulo of the source IP address of the ARP request.

After the end host receives the ARP response from the gateway, it caches the MAC address and all traffic from the host is routed via the firewall that responded with the virtual MAC address for the lifetime of the ARP cache. The lifetime of the ARP cache depends on the end host operating system.

upvoted 1 times

  **djedeen** 1 year, 7 months ago

Selected Answer: B

B; one floating IP per firewall, moved around via gratuitous ARP upon failure.



upvoted 2 times

  **Bobhope** 1 year, 7 months ago

Selected Answer: B

VickiF is correct. The docs say that each HA interface has its own IP and floating IP. That makes two floating IPs. Answer A says there is only one shared IP and is thus false.

upvoted 2 times

  **VickiF** 1 year, 7 months ago

Selected Answer: B

It should be B. Each firewall has its own floating IP, so that traffic can flow to both. When something happens to one firewall, its floating IP will failover to the other firewall, and that firewall will have both floating IPs.

upvoted 2 times

Which version of GlobalProtect supports split tunneling based on destination domain, client process, and HTTP/HTTPS video streaming application?

- A. GlobalProtect version 4.0 with PAN-OS 8.1
- B. GlobalProtect version 4.1 with PAN-OS 8.1
- C. GlobalProtect version 4.1 with PAN-OS 8.0
- D. GlobalProtect version 4.0 with PAN-OS 8.0

Correct Answer: B

Reference:

https://www.paloaltonetworks.com/documentation/41/globalprotect/globalprotect-app-new-features/new-features-released-in-gp-agent-4_1/split-tunnel-for-public-applications

  **whiteherondance** Highly Voted 2 years, 6 months ago

I can't believe this is a question lol
upvoted 23 times

  **zadkiel** Highly Voted 4 years, 1 month ago

correct B
upvoted 11 times

  **Marshpillowz** Most Recent 7 months, 1 week ago



Selected Answer: B

B is correct
upvoted 1 times

  **Sammy3637** 8 months, 4 weeks ago

Selected Answer: B

Outdated , all the versions after 8.1 also support
upvoted 2 times

  **kewokil120** 1 year, 5 months ago

Selected Answer: B

B is the answer
upvoted 1 times

How does Panorama prompt VMWare NSX to quarantine an infected VM?

- A. HTTP Server Profile
- B. Syslog Server Profile
- C. Email Server Profile
- D. SNMP Server Profile

Correct Answer: A

Reference:

<https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization/set-up-the-vm-series-firewall-on-vmware-nsx/dynamically-quarantine-infected-guests>

  **mattass** Highly Voted 4 years, 3 months ago

Panorama includes predefined payload formats for threat and traffic logs in the HTTP Server Profile. These payload formats correspond to predefined security tags in NSX-V. When a guest VM is found in the threat or traffic logs, Panorama makes an API call to NSX-V Manager telling NSX-V Manager to tag the guest VM with the tag specified in the HTTP Server Profile. When the guest VM becomes tagged, NSX-V Manager dynamically moves the tagged guest VM into the quarantine security group, which places the guest VM into the quarantine dynamic address group.

upvoted 11 times

  **yoginangpal** Highly Voted 3 years, 3 months ago

A is correct and here is the updated reference:

<https://docs.paloaltonetworks.com/vm-series/10-0/vm-series-deployment/set-up-the-vm-series-firewall-on-nsx/set-up-the-vm-series-firewall-on-vmware-nsx/dynamically-quarantine-infected-guests.html#id8e9a242e-e038-4ba2-b0ea-aaaf53690be0>

upvoted 6 times

  **scanossa** Most Recent 7 months ago

Selected Answer: A

According to the links provided here, the answer is HTTP Server profile

upvoted 1 times

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: A

Answer is A

upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/vm-series/10-0/vm-series-deployment/set-up-the-vm-series-firewall-on-nsx/set-up-the-vm-series-firewall-on-vmware-nsx/dynamically-quarantine-infected-guests>

upvoted 2 times

  **ChiaPet75** 4 years, 2 months ago

Agreed. The correct answer is "A" and this applies for both NSX-V and NSX-T.

upvoted 5 times

An administrator accidentally closed the commit window/screen before the commit was finished. Which two options could the administrator use to verify the progress or success of that commit task? (Choose two.)

A.

The screenshot shows the Palo Alto Networks GUI with the 'Monitor' tab selected. The left sidebar lists various log categories, and the main area displays a table of system logs. The logs include events such as user logins, authentication successes, and database upgrades.

Receive Time	Type	Severity	Event	Object	Description
06/16 08:41:43	general	informational	general		User admin accessed Monitor tab.
06/16 08:40:40	general	informational	general		User admin logged in via Web from 192.168.55.1 using https.
06/16 08:40:40	auth	informational	auth-success		authenticated for user 'admin'. From: 192.168.55.1.
06/16 08:40:06	general	informational	general		LOGIN ON tty1 BY admin.
06/16 08:39:43	general	informational	general		User admin logged in via CLI from Console.
06/16 08:39:42	auth	informational	auth-success		authenticated for user 'admin'. From: (null).
06/16 08:39:16	url-filtering	informational	upgrade-url-database-success		PAN-DB was upgraded to version 20170615.40151.
06/16 08:34:15	url-filtering	informational	upgrade-url-database-success		PAN-DB was upgraded to version 20170615.40150.
06/16 08:31:44	general	informational	general		Failed to connect to Panorama Server: 192.168.55.5 Port: 3978 Retry: 0
06/16 08:31:40	ntpd	informational	restart		NTP restart synchronization performed
06/16 08:31:33	general	informational	general		Commit job succeeded. Completion time=2017/06/16 05:31:33. JobId=29. User:admin

B.

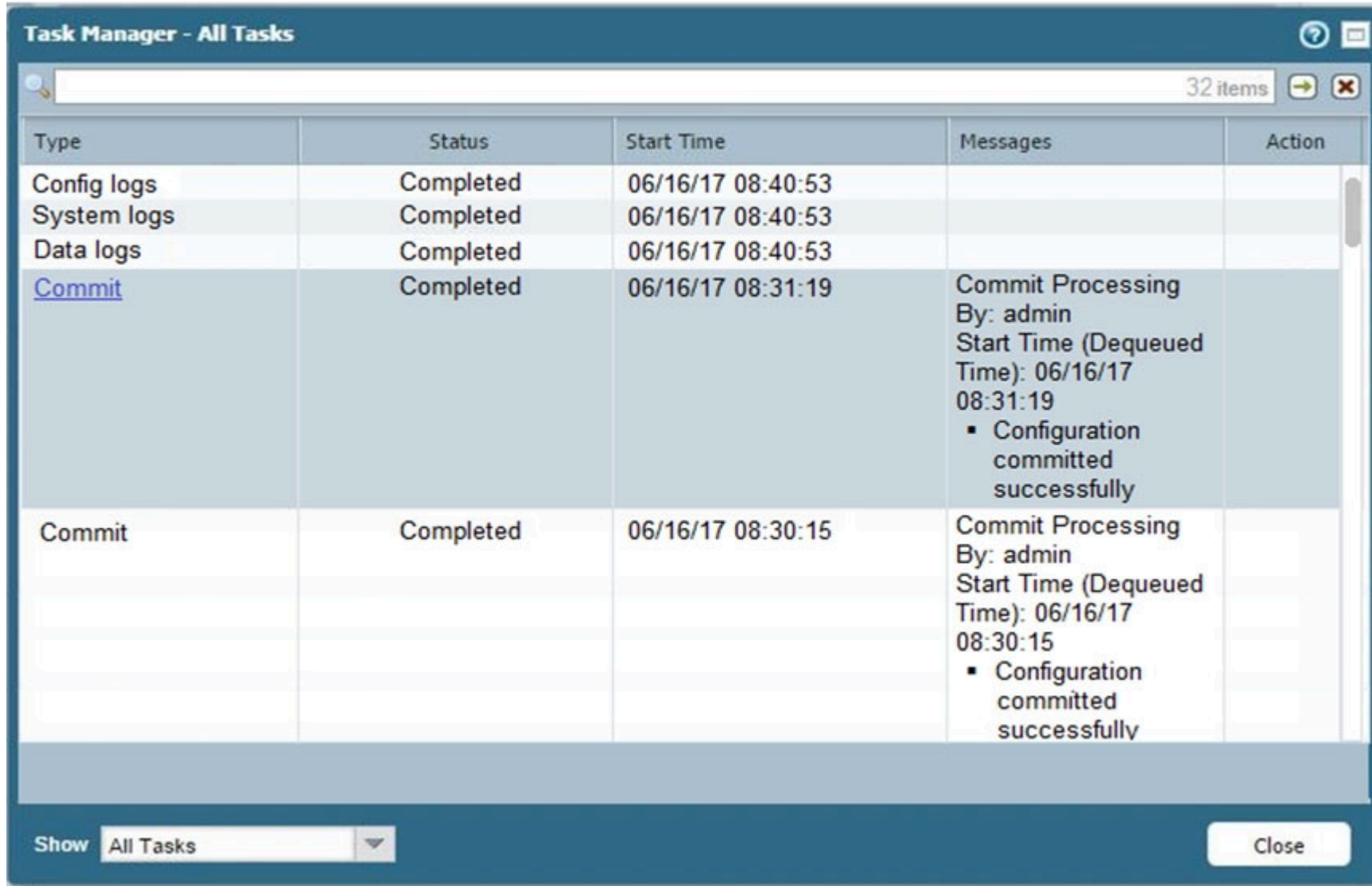
The screenshot shows the Palo Alto Networks GUI with the 'Monitor' tab selected. The left sidebar lists various log categories, and the main area displays a table of traffic logs. The logs show network traffic events with details on receive time, type, zones, source, and destination.

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination
06/14 08:14:14	end	inside	outside	192.168.45.1		192.168.45.255
06/14 08:13:44	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 08:04:14	end	inside	outside	192.168.45.1		192.168.45.255
06/14 08:03:45	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:59:36	end	inside	outside	192.168.45.1		192.168.45.255
06/14 07:59:06	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:40:27	end	inside	outside	192.168.45.1		192.168.45.255
06/14 07:39:57	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:39:56	drop	outside	outside	192.168.55.1		192.168.55.255
06/14 07:39:55	drop	outside	outside	192.168.55.1		192.168.55.255

C.

05/23 20:49:30	port	informational	link-change	ethernet1/1	Port ethernet1/1: Down 10Gb/s-full duplex
05/23 20:49:29	port	high	link-change	MGT	Port MGT: Down 1Gb/s Full duplex
05/23 20:47:24	port	informational	link-change	ethernet1/1	Port ethernet1/1: Up 10Gb/s-full duplex
05/23 20:47:22	port	informational	link-change	MGT	Port MGT: Up Unknown
05/23 20:47:18	port	informational	link-change	ethernet1/1	Port ethernet1/1: Down 10Gb/s-full duplex
05/23 20:47:17	port	high	link-change	MGT	Port MGT: Down 1Gb/s Full duplex

D.



Correct Answer: AD

- trashboat** Highly Voted 3 years, 4 months ago

A & D are correct, also you can use the command 'show jobs all' and find the commit job, then you could use 'show jobs id <id>' to show only that commit job process.

upvoted 17 times
- Marshpillowz** Most Recent 7 months, 1 week ago

A and D correct

upvoted 1 times
- kewokil120** 1 year, 5 months ago

Ad is the answer

upvoted 1 times
- lol12** 1 year, 10 months ago

AD

trashboat is correct.

Can't be B as that's just traffic logs and C is interface info.

upvoted 2 times

Which two actions would be part of an automatic solution that would block sites with untrusted certificates without enabling SSL Forward Proxy?
(Choose two.)

- A. Create a no-decrypt Decryption Policy rule.
- B. Configure a Dynamic Address Group for untrusted sites.
- C. Create a Security Policy rule with a vulnerability Security Profile attached.
- D. Enable the "Block sessions with untrusted issuers" setting.

Correct Answer: AD

  **TAKUM1y** Highly Voted  1 year, 10 months ago



Selected Answer: AD

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-concepts/no-decryption-decryption-profile>
upvoted 6 times



  **Marshpillowz** Most Recent  7 months, 1 week ago

Selected Answer: AD

A and D correct
upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

Agree that it is A & D.
upvoted 1 times

  **lol12** 1 year, 10 months ago

Agree AD
upvoted 3 times

  **CCIE5592** 1 year, 11 months ago

A and D are correct. <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-concepts/no-decryption-decryption-profile>
upvoted 3 times



An administrator is defining protection settings on the Palo Alto Networks NGFW to guard against resource exhaustion. When platform utilization is considered, which steps must the administrator take to configure and apply packet buffer protection?

- A. Enable and configure the Packet Buffer Protection thresholds. Enable Packet Buffer Protection per ingress zone.
- B. Enable and then configure Packet Buffer thresholds. Enable Interface Buffer protection.
- C. Create and Apply Zone Protection Profiles in all ingress zones. Enable Packet Buffer Protection per ingress zone.
- D. Configure and apply Zone Protection Profiles for all egress zones. Enable Packet Buffer Protection per egress zone.
- E. Enable per-vsys Session Threshold alerts and triggers for Packet Buffer Limits. Enable Zone Buffer Protection per zone.

Correct Answer: A

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/zone-protection-and-dos-protection/configure-zone-protection-to-increase-network-security/configure-packet-buffer-protection>

  **bmarks** Highly Voted 3 years, 6 months ago

Answer = A

The following excerpts from 9.1 Docs confirm the answer:

... Packet Buffer Protection defends ingress zones.

... you don't configure Packet Buffer Protection in a Zone Protection profile

... tune the Packet Buffer Protection thresholds

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense/packet-buffer-protection.html>

upvoted 5 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: A

Answer is A

upvoted 1 times

  **lol12** 1 year, 10 months ago

Selected Answer: A

A

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/configure-zone-protection-to-increase-network-security/configure-packet-buffer-protection>

upvoted 3 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: A

<https://live.paloaltonetworks.com/t5/%E5%85%AC%E5%85%B1%E5%B8%82%E5%A0%B4%E5%90%91%E3%81%91%E6%83%85%E5%A0%B1/%E6%98%A8%E4%BB%8A%E3%81%AEdos%E6%94%BB%E6%92%83%E3%81%AE%E5%82%BE%E5%90%91%E3%81%A8pa%E3%82%B7%E3%83%AA%E3%83%BC%E3%82%BA%E3%81%AEdos%E9%98%B2%E5%BE%A1%E6%A9%9F%E8%83%BD%E3%81%AE%E4%BD%BF%E3%81%84%E6%96%B9/ta-p/407688>

upvoted 3 times

  **nicolasjiang** 4 years, 1 month ago

correct a

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/zone-protection-and-dos-protection/configure-zone-protection-to-increase-network-security/configure-packet-buffer-protection>

upvoted 3 times

  **rammsdoct** 4 years, 3 months ago

A:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/zone-protection-and-dos-protection/configure-zone-protection-to-increase-network-security/configure-packet-buffer-protection>

upvoted 4 times

  **Ab121213** 4 years, 3 months ago

Sounds like D to me :

Same web link :

Enable packet buffer protection on an ingress zone.

Select Network

Zones


.

Choose an ingress zone and click on its name.

Select the Enable Packet Buffer Protection

check box in the Zone Protection section.
Click OK

upvoted 1 times

  **jpm_1506** 3 years, 8 months ago

"A" is correct. you dont need a ZPF at all to have buffer protection enabled on a zone. and will be per zone on ingress as per life of a packet.
upvoted 3 times

Question #148

Topic 1

What is the purpose of the firewall decryption broker?

- A. decrypt SSL traffic and then send it as cleartext to a security chain of inspection tools.
- B. force decryption of previously unknown cipher suites
- C. reduce SSL traffic to a weaker cipher before sending it to a security chain of inspection tools.
- D. inspect traffic within IPsec tunnels

Correct Answer: A

Reference:

<https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/decryption-features/decryption-broker>

  **rammsdoct** Highly Voted 4 years, 2 months ago

A:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-new-features/decryption-features/decryption-broker>

upvoted 10 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

  **aatechler** 1 year, 10 months ago

Selected Answer: A

This feature will decrypt traffic and forward it out of the selected interface to a specific security device or service (or chain of devices) that examines the cleartext traffic.

The last service in the chain returns the packet to the firewall, which then encrypts it and forwards it to the original destination.


upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/decryption-broker/decryption-broker-how-it-works#id182QLM00OH2>

upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: A

A is a correct answer

upvoted 2 times

SAML SLO is supported for which two firewall features? (Choose two.)

- A. GlobalProtect Portal
- B. CaptivePortal
- C. WebUI
- D. CLI

Correct Answer: AC

Reference:

<https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-saml-authentication>

  **santino** Highly Voted 4 years, 3 months ago

Agree with Anoopmp: A and C

SSO is available to administrators who access the web interface and to end users who access applications through GlobalProtect or Captive Portal.

SLO is available to administrators and GlobalProtect end users, but not to Captive Portal end users.



<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/authentication/authentication-types/saml>
upvoted 16 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: AC

A and C correct

upvoted 1 times

  **lol12** 1 year, 10 months ago


Selected Answer: AC

AC

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/authentication/configure-saml-authentication>

SLO is available to administrators and GlobalProtect end users, but not to Authentication Portal end users.

upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: AC

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/authentication/configure-saml-authentication>

upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: AC

A and C. Not B!!!!

Don't mess SSO and SLO:

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/authentication/configure-saml-authentication>

SSO is available to administrators and to GlobalProtect and Authentication Portal end users. SLO is available to administrators and GlobalProtect end users, but not to Authentication Portal end users.

Administrators can use SAML to authenticate to the firewall web interface, but not to the CLI.



upvoted 2 times

  **AbuHussain** 2 years, 5 months ago

Selected Answer: AC

A and C.

upvoted 3 times

  **Zabol** 3 years, 2 months ago

I am using SAML SLO for production Firewall, and it is definitely Global Protect and WebUI

upvoted 2 times

  **yoginangpal** 3 years, 3 months ago

Correct answer is AC this should be corrected

upvoted 2 times

  **trashboat** 3 years, 4 months ago

A & C are correct:

"You cannot enable SLO for Authentication (Captive) Portal users."

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-web-interface-help/device/device-server-profiles-saml-identity-provider>
upvoted 3 times

  **aadach** 3 years, 5 months ago



AC ! , Ive just checked it on my fw (panos v10)
upvoted 3 times

  **PNARESHA** 3 years, 6 months ago

A and C. (its SLO)

SSO is available to administrators who access the web interface and to end users who access applications through GlobalProtect or Captive Portal.
SLO is available to administrators and GlobalProtect end users, but not to Captive Portal end users.

upvoted 1 times

  **Sarbi** 3 years, 9 months ago

A and c is the correct.
\Administrators cannot use SAML to authenticate to the CLI on the firewall or Panorama.
You cannot use SAML authentication profiles in authentication sequences.



upvoted 2 times

  **Anoopmp** 4 years, 3 months ago

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/authentication/authentication-types/saml>
upvoted 2 times

  **Anoopmp** 4 years, 3 months ago

Correct answer is A and C
upvoted 2 times

  **bakkar** 4 years, 3 months ago

Answer is A C,
<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/authentication/authentication-types/saml>
upvoted 1 times

  **TamerRouby** 4 years, 3 months ago

A, C are the correct answer as it is saying SLO, not SSO

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/authentication/configure-saml-authentication>
<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/configure-saml-authentication.html>
upvoted 4 times

What are the two behavior differences between Highlight Unused Rules and the Rule Usage Hit counter when a firewall is rebooted? (Choose two.)

- A. Rule Usage Hit counter will not be reset.
- B. Highlight Unused Rules will highlight all rules.
- C. Highlight Unused Rules will highlight zero rules.
- D. Rule Usage Hit counter will reset.

Correct Answer: AB

Anoopmp Highly Voted 4 years, 3 months ago

Correct Answer A and C.
upvoted 10 times

ChiaPet75 Highly Voted 4 years, 2 months ago

Correct: A,B

(Per PANOS Help Function) - Each firewall maintains a traffic flag for the rules that have a match. Because the flag is reset when a dataplane reset occurs on a reboot or a restart, it is best practice to monitor this list periodically to determine whether the rule had a match since the last check before you delete or disable it.

This mean when the dataplane is reset or there is a reboot the flag will not be set for any security policies therefore they will all be highlighted until a rule is hit and the flag is set.

upvoted 10 times

Marshpillowz Most Recent 7 months, 1 week ago

Selected Answer: AB

A and B correct
upvoted 1 times

DatITGuyTho1337 8 months, 2 weeks ago

D is definitely part of the answer because the rule usage counter always resets following firewall reboot.
upvoted 1 times

DatITGuyTho1337 8 months, 2 weeks ago

Nevermind, found the following line from one of the articles: "Hit Count—The number of times traffic matched the criteria you defined in the policy rule. Persists through reboot, dataplane restarts, and upgrades unless you manually reset or rename the rule."

upvoted 1 times

Xuzi 9 months, 3 weeks ago

Selected Answer: AB

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVICA0>
upvoted 1 times

Micutzu 10 months ago

Selected Answer: AB

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVICA0>
upvoted 1 times

gc999 10 months, 1 week ago

Selected Answer: A

Only "A" is definitely correct.

The fact is "Rule Usage Hit Counter will not be reset", it is proven from the lab. Then:

1. "A" - must always be correct
2. "B" - since Hit Count NOT be reset, it would not "all" rules are unused. (Maybe some are unused, i.e. no hit count, but it already happened before reboot)
3. "D" - must always be wrong
4. "C" - It depends. As mentioned on "2" above, maybe some rules are unused before reboot, so "some" rules already have ZERO hit count before reboot.

upvoted 1 times

alinio11 1 year, 1 month ago

I've just tested in my LAB: Is A&C. If I had the option to paste here the printscreen , I would do it.
upvoted 1 times

  **gc999** 10 months, 1 week ago

The question is not good. I agree with A only. If the question is with wording "assume all rules are not zero in hit counter before reboot ...", then I will also go with "C"

upvoted 1 times

  **duckduckgoo** 1 year, 3 months ago

Selected Answer: AB

FOr people thinking it's C, take a look at the link below. "Notice how the rules looks after selecting "Highlight Unused Rules." You can now see exactly what rules have and have not been used since the last reboot. "



<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVICA0>

upvoted 1 times

  **lildevil** 1 year, 5 months ago

A & B with out question. To all who said answer C...what would happen if a rule is created but never been hit? Of course it would be highlighted so C could never be correct.

upvoted 1 times

  **dogeatdog** 1 year, 8 months ago

Selected Answer: AB

A and B. Be careful of the wording. this is a double negative. Cisco uses this trickery also.

upvoted 3 times

  **lol12** 1 year, 10 months ago

Selected Answer: AB

Can't be C. If you have a running firewall with a rule that has not been used then it will be highlighted. If we reboot the appliance then - given there was no traffic - all rules will be highlighted. If zero rules would be highlighted then it means every rule was used...

upvoted 3 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: AC

A: <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/view-policy-rule-usage>

C: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVICA0>

upvoted 2 times

  **DenskyDen** 1 year, 7 months ago

Based on the article posted, it should be A and B.

upvoted 2 times

  **Pretorian** 2 years ago

I agree with A and B but what are the chances that after a reboot, you will check that box before packets hit one or many of the rules?

upvoted 3 times

  **eyelasers1** 2 years, 6 months ago

Answer: AB

"Hit Count—The number of times traffic matched the criteria you defined in the policy rule. Persists through reboot, dataplane restarts, and upgrades unless you manually reset or rename the rule."

Source: <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/view-policy-rule-usage.html>

"Notice how the rules looks after selecting "Highlight Unused Rules." You can now see exactly what rules have and have not been used since the last reboot. The red boxes around the rules have been added to show you how the "highlight" feature works."

Source: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVICA0>

upvoted 6 times

  **NNgiggs** 2 years, 7 months ago

The Right answer is AB, the question is so complicated but what they are looking for is to know if you Understand that highlight unused rules will highlight all unused since the last reboot as opposed to hit count which does not change after a reboot. See link below and read the notice below the second picture.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVICA0>

upvoted 4 times

  **GivemeMoney** 2 years, 7 months ago

Selected Answer: AB

Rule usage hit counter will only reset if you manually reset them.
Highlight unused rules will highlight all rules if not used since start.

upvoted 2 times

Which is not a valid reason for receiving a decrypt-cert-validation error?

- A. Unsupported HSM
- B. Unknown certificate status
- C. Client authentication
- D. Untrusted issuer

Correct Answer: A

Reference:

<https://www.paloaltonetworks.com/documentation/71/pan-os/newfeaturesguide/networking-features/ssl-ssh-session-end-reasons>

  **ChiaPet75** Highly Voted 4 years, 2 months ago

Correct: A

The question reads, "Which is NOT a valid reason for receiving a decrypt-cert-validation error?"

Per the link "hamshoo" provided, receiving the decrypt-cert-validation error is valid for the following conditions: expired, untrusted issuer, unknown status, or status verification time-out. "Unsupported HSM" is not a valid reason for receiving a decrypt-cert-validation error.

upvoted 19 times

  **swajal** Highly Voted 4 years, 2 months ago

Option 'A' Should be the answer as the question says "what is not a valid reason". HSM is not the valid reason

upvoted 9 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: A

Correct answer is A

upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/troubleshoot-and-monitor-decryption/decryption-logs/decryption-log-errors-and-error-indexes>

upvoted 2 times

  **yoginangpal** 3 years, 3 months ago

To not to trick people they should put NOT in uppercase in the question, I am not sure what is the point of trying to ask tricky questions!

upvoted 3 times

  **PuckinWebGuy** 3 years, 6 months ago

decrypt-cert-validation error would appear for SSL Forward Proxy. HSM is used to hold the private key for SSL Inbound Inspection, so an HSM issue is NOT a valid reason.

Answer is A.

upvoted 4 times

  **rammsdoct** 4 years, 2 months ago

@Hamshoo, yes you are right I was thinking about HSM (Hardware security module), but then read the question very carefully and it said "decrypt cert validation" which one of the options is untrusted issuer, so yes D is right!

upvoted 3 times

  **hamshoo** 4 years, 2 months ago

Answer is D:

<https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-new-features/networking-features/ssl-ssh-session-end-reasons>

upvoted 2 times

In the following image from Panorama, why are some values shown in red?

Device Name	Logging Rate (Log/sec)	Device	Session
		Throughput (KB/sec)	Count (Sessions)
uk3	781	209	40221
sg2	0	953	170
us3	291	0	67455

- A. sg2 session count is the lowest compared to the other managed devices.
- B. us3 has a logging rate that deviates from the administrator-configured thresholds.
- C. uk3 has a logging rate that deviates from the seven-day calculated baseline.
- D. sg2 has misconfigured session thresholds.

Correct Answer: C

Reference:

<https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/panorama-features/device-monitoring-through-panorama>

Marshpillowz 7 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

BryanSalazar 1 year, 5 months ago

Selected Answer: C

The answer which makes the most sense is C, however I believe the questions is not properly worded.

"In the following image from Panorama, why are some values shown in red?"

C. uk3 has a logging rate that deviates from the seven-day calculated baseline.

The values that are red are not red due to uk3 being a deviating device. A more adequate correct answer would be "Because the devices are deviating from the seven-day calculated baseline."

upvoted 2 times

lol12 1 year, 10 months ago

Selected Answer: C

Answer C

Panorama > Managed Devices > Health > Deviating Devices

The Deviating Devices tab displays devices that have any metrics that are deviating from their calculated baseline and displays those deviating metrics in red. A metric health baseline is determined by averaging the health performance for a given metric over seven days plus the standard deviation.

upvoted 2 times

TAKUM1y 1 year, 10 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-managed-devices-summary/panorama-managed-devices-health>

upvoted 2 times

UFanat 2 years, 2 months ago

Selected Answer: C

C is a correct one.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/panorama-web-interface/panorama-managed-devices-summary/panorama-managed-devices-health>

A metric health baseline is determined by averaging the health performance for a given metric over seven days plus the standard deviation.

upvoted 1 times

Scryptre 2 years, 9 months ago

but how the 7-day is obtained? Why is it not B) .. deviates from the administrator-configured thresholds ?



upvoted 1 times

gaven186 3 years, 1 month ago

Answer C.

"The Deviating Devices tab displays devices that have any metrics that are deviating from their calculated baseline and displays those deviating metrics in red. A metric health baseline is determined by averaging the health performance for a given metric over seven days plus the standard deviation."

upvoted 1 times

  **mmed** 3 years, 5 months ago

Confirm C

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/panorama-web-interface/panorama-managed-devices-summary/panorama-managed-devices-health>

upvoted 3 times

The firewall is not downloading IP addresses from MineMeld. Based on the image, what most likely is wrong?

- A. A Certificate Profile that contains the client certificate needs to be selected.
- B. The source address supports only files hosted with an ftp://<address/file>.
- C. External Dynamic Lists do not support SSL connections.
- D. A Certificate Profile that contains the CA certificate needs to be selected.

Correct Answer: D

Reference:

<https://live.paloaltonetworks.com/t5/MineMeld-Articles/Connecting-PAN-OS-to-MineMeld-using-External-Dynamic-Lists/ta-p/190414>

Marshpillowz 7 months, 1 week ago

Selected Answer: D

D appears to be correct
upvoted 1 times

djeden 1 year, 7 months ago

Selected Answer: D

D:
First thing, download the certificate of the CA of the AutoFocus/MineMeld SSL certificate from the following link:
<https://certs.godaddy.com/repository/gd-class2-root.crt>
upvoted 4 times

Prutser2 3 years, 2 months ago

common sense question, so D
upvoted 1 times

habualrob 3 years, 2 months ago

the answer is D
upvoted 2 times

kraut 3 years, 4 months ago

D is valid choice

I set this up just today (Pan-OS 9.1). It works perfectly without a cert profile BUT since this is sensitive data you should add a cert profile. this enables the firewall to verify whom it's talking to.

upvoted 1 times

bloodtech 3 years, 5 months ago

D - "If the list source is secured with SSL (i.e. lists with an HTTPS URL), enable server authentication. Select a Certificate Profile or create a New Certificate Profile for authenticating the server that hosts the list. The certificate profile you select must have root certificate authority (CA) and intermediate CA certificates that match the certificates installed on the server you are authenticating."

upvoted 4 times

Which three split tunnel methods are supported by a GlobalProtect Gateway? (Choose three.)

- A. video streaming application
- B. Client Application Process
- C. Destination Domain
- D. Source Domain
- E. Destination user/group
- F. URL Category



Correct Answer: ABC

Reference:

<https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/globalprotect-features/split-tunnel-for-public-applications>

- [-] **rammsdoct** Highly Voted 4 years, 2 months ago
<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-new-features/globalprotect-features/split-tunnel-for-public-applications.html>
ABC
upvoted 10 times
- [-] **Marshpillowz** Most Recent 7 months, 1 week ago
Selected Answer: ABC
A, B and C correct
upvoted 1 times
- [-] **joquin0020** 9 months ago
Selected Answer: ABC
I DID HIS TODAY
upvoted 1 times
- [-] **Kjohnsting** 1 year, 7 months ago
Client app process???
upvoted 3 times
- [-] **DenskyDen** 1 year, 7 months ago
Selected Answer: ABC
You can configure split tunnel traffic based on an access route, destination domain, application, and HTTP/HTTPS video streaming application.
upvoted 1 times
- [-] **lol12** 1 year, 10 months ago
Selected Answer: ABC
ABC
<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-gateways/split-tunnel-traffic-on-globalprotect-gateways>
You can configure split tunnel traffic based on an access route, destination domain, application, and HTTP/HTTPS video streaming application.
upvoted 2 times
- [-] **TAKUM1y** 1 year, 10 months ago
Selected Answer: ABC
<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-gateways/split-tunnel-traffic-on-globalprotect-gateways>
upvoted 2 times
- [-] **UFanat** 2 years, 2 months ago
Selected Answer: ABC
you can exclude by domain, process name or video streaming apps
upvoted 1 times
- [-] **NLT** 2 years, 6 months ago
Software Support: Starting with GlobalProtect™ App 4.1 and with PAN-OS® 8.1 and later releases
OS Support: Windows 7 Service Pack 2 and later releases and macOS 10.10 and later releases
In addition to route-based split tunneling, the GlobalProtect app for Windows and macOS endpoints now supports split tunneling based on destination domain, client process, and HTTP/HTTPS video streaming application.

upvoted 2 times

  **bmarks** 3 years, 6 months ago

Answer = ABC

You can configure split tunnel traffic based on an access route, destination domain, application, and HTTP/HTTPS video streaming application.

<https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin/globalprotect-gateways/split-tunnel-traffic-on-globalprotect-gateways.html>

upvoted 4 times

Which two are valid ACC GlobalProtect Activity tab widgets? (Choose two.)

- A. Successful GlobalProtect Deployed Activity
- B. GlobalProtect Deployment Activity
- C. Successful GlobalProtect Connection Activity
- D. GlobalProtect Quarantine Activity

Correct Answer: BC

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/globalprotect-features/enhanced-logging-for-globalprotect.html>

  **petersummer** Highly Voted 3 years, 5 months ago

In PAN OS 10.0 correct answers are B, C, D. Checked in Panorama right now
upvoted 13 times

  **Elvenking** 2 years, 4 months ago

In Pan-OS 10.1 B,C,D are correct as well
upvoted 4 times

  **aatechler** Highly Voted 1 year, 7 months ago

It includes the following:-
Successful GlobalProtect Connection Activity
Unsuccessful GlobalProtect Connection Activity
GlobalProtect Deployment Activity
GlobalProtect Quarantine Activity
upvoted 6 times

  **327c7c8** Most Recent 5 months, 1 week ago



Selected Answer: CD

B,C and D
I am fed up with this bad practice exam
upvoted 3 times

  **Marshpillowz** 7 months, 1 week ago


Selected Answer: BC

B, C and D correct
upvoted 2 times


  **JRKhan** 7 months, 3 weeks ago

Selected Answer: BC

For PANOS 9 and 10.1(as well), BC are correct. The third option is Unsuccessful GlobalProtect Connection Activity.
upvoted 1 times

  **UTF** 1 year, 4 months ago

B & C NOTICE the word ACTIVITY in the Question. That removed the Quarantine option even though it is present. It is not an Activity widget.
upvoted 2 times

  **Pochex** 1 year, 6 months ago



In PANOS 10.1 B, C, and D are available. I accessed the WebUI to confirm.
upvoted 2 times

  **Kjohnsting** 1 year, 7 months ago

This one needs updating
upvoted 3 times

  **gully300** 1 year, 7 months ago

PAN OS 10.1
<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/logging-for-globalprotect-in-pan-os/view-a-graphical-display-of-globalprotect-user-activity-in-pan-os>
upvoted 1 times

  **lol12** 1 year, 10 months ago

Selected Answer: BC

BC

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/globalprotect-features/enhanced-logging-for-globalprotect>

Available options from admin guide:
Successful GlobalProtect Connection Activity
Unsuccessful GlobalProtect Connection Activity
GlobalProtect Deployment Activity

upvoted 1 times

[-]  **TAKUM1y** 1 year, 10 months ago

Selected Answer: BCD

<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/logging-for-globalprotect-in-pan-os/view-a-graphical-display-of-globalprotect-user-activity-in-pan-os>

upvoted 4 times

[-]  **secdaddy** 1 year, 11 months ago

Maybe an outdated question but if it comes up then arguably BD is the 'better' answer as it works pre-10 as well.

upvoted 1 times

[-]  **GheeHong** 2 years, 1 month ago

If only refer to this dump, you will not able to pass the PCNSE exam.
Any alternate source recommend?

upvoted 1 times

[-]  **UFanat** 2 years, 2 months ago

Selected Answer: BC

BC but D is also correct since PanOS 10.0

upvoted 2 times

[-]  **lucaboban** 3 years, 5 months ago

BD is correct answer as per PANOS 10

upvoted 1 times

[-]  **gordonF** 3 years, 6 months ago

Yes, b and c are correct. But from PA v10, D is also.

upvoted 1 times

[-]  **bmarks** 3 years, 6 months ago

PCNSE 9 focuses solely on PANOS 9.1

upvoted 2 times

Which two features can be used to tag a username so that it is included in a dynamic user group? (Choose two.)

- A. log forwarding auto-tagging
- B. XML API
- C. GlobalProtect agent
- D. User-ID Windows-based agent

Correct Answer: *BD*

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups.html>

  **PuckinWebGuy** Highly Voted 3 years, 6 months ago

From the PCNSE study guide, Dynamic User Groups (page 106):

Username also can be tagged and untagged using the autotagging feature in a Log Forwarding Profile. You also can program another utility to invoke PAN-OS XML API commands to tag or untag usernames. In the web interface you can use logical AND or OR operators with the tags to better filter or match against. You can configure a timeout value that determines when a username will be untagged automatically.

Based on that paragraph, A&B are the correct answers.

upvoted 32 times

  **MS_NW** Highly Voted 4 years, 1 month ago

BD

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups.html>

To dynamically register tags, you can use:

the XML API

the User-ID agent

Panorama

the web interface on the firewall

upvoted 14 times

  **Chiquitabandita** 7 months, 1 week ago

On that same link though: The firewall redistributes the tags for the dynamic user group to the next hop and you can configure log forwarding to send the logs to a specific server. Log forwarding also allows you to use auto-tagging to automatically add or remove members of dynamic user groups based on events in the logs.

upvoted 1 times

  **Gabbranch** 9 months, 1 week ago

The UserID agent referenced is Panorama and Data Redistribution, not the Windows agent.



upvoted 1 times

  **apiloran** Most Recent 1 month, 2 weeks ago

Selected Answer: AB

A&B are the correct answers

upvoted 2 times

  **123XYZT** 3 months, 3 weeks ago

A and B

From PCNSE-Study-Guide

Username also can be tagged and untagged using the auto-tagging feature in a Log Forwarding Profile. You also can program another utility to invoke PAN-OS XML API commands to tag or untag usernames.

upvoted 3 times

  **Andromeda1800** 8 months, 3 weeks ago

Selected Answer: AB

I think confusion comes from mixing two different "tools" 1. auto-tagging users to include them in DUG and 2. dynamically register tags. Those are two different operations.

-to auto-tag users to DUG:

auto-tagging in log-forwarding,

XML API

-to dynamically add tags:

XML API, Panorama, User-ID

-to statically add tags:

WebUI

upvoted 6 times

  **RoamingFo** 9 months, 2 weeks ago

Selected Answer: AB

On one side the study guide and the doc referred below confirm about the XML API & the Log Forwarding Profile Auto-Tagging. On the other side, the User-ID agent mentioned on the below document, refer to the Panorama User-ID agent and Remote-Firewall User-ID agent, in other words the redistribution agents "Step 6 -2"

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/use-dynamic-user-groups-in-policy>

upvoted 3 times

Gabranch 9 months, 1 week ago

Agreed - Documentation talks about Panorama UserID agent being used for tagging. But not Windows UserID Agent.

upvoted 1 times

Xuzi 9 months, 4 weeks ago

Selected Answer: BD

B-D

the XML API

the User-ID agent

upvoted 1 times

Redrum702 1 year, 2 months ago

BD are correct

upvoted 1 times

[Removed] 1 year, 5 months ago

Selected Answer: BD

b and d sorry

upvoted 2 times

[Removed] 1 year, 5 months ago

Selected Answer: BD

a d are correct

upvoted 1 times

Pochex 1 year, 6 months ago

B and D are correct. To dynamically register tags, you can use:

- the XML API
- the User-ID agent
- Panorama
- the web interface on the firewall

Please refer to <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/use-dynamic-user-groups-in-policy>

upvoted 1 times

Eldaby 1 year, 5 months ago

there are new questions about PAN OS 11, do you have them?

upvoted 1 times

mohr22 1 year, 6 months ago

Its B and D

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/use-dynamic-user-groups-in-policy>

upvoted 3 times

Mauz88 1 year, 6 months ago

On PAN-OS 10.1 the options are:

To dynamically register tags, you can use:

the XML API

the User-ID agent

Panorama

the web interface on the firewall

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/use-dynamic-user-groups-in-policy>

upvoted 2 times

mohr22 1 year, 7 months ago

B and DTo dynamically register tags, you can use:

the XML API

the User-ID agent

Panorama

the web interface on the firewall

upvoted 2 times

bearfromdownunder 1 year, 7 months ago

Selected Answer: BD

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups>

upvoted 3 times

  **awtsuriticuna** 1 year, 9 months ago



B/D

To dynamically register tags, you can use:

the XML API
the User-ID agent
Panorama
the web interface on the firewall

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups>

upvoted 2 times

  **lazyy** 1 year, 9 months ago

Selected Answer: BD

See comment of MS_NW

BD

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups.html>

To dynamically register tags, you can use:

the XML API
the User-ID agent
Panorama
the web interface on the firewall

upvoted 3 times

SD-WAN is designed to support which two network topology types? (Choose two.)

- A. point-to-point
- B. hub-and-spoke
- C. full-mesh
- D. ring

Correct Answer: BC

—  **jordan_gsi** Highly Voted 3 years, 5 months ago

SD-WAN supports a full mesh topology, in addition to the hub-spoke topology. The mesh can consist of branches with or without hubs. Use full mesh when the branches need to communicate with each other directly.

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/sd-wan-features/sd-wan-full-mesh-vpn-cluster-with-ddns-service.html>

BC

upvoted 8 times

—  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: BC

B and C correct

upvoted 1 times

—  **lol12** 1 year, 10 months ago

Selected Answer: BC

BC

<https://docs.paloaltonetworks.com/sd-wan/3-0/sd-wan-admin/configure-sd-wan/create-a-vpn-cluster>

upvoted 2 times

—  **TAKUM1y** 1 year, 10 months ago

Selected Answer: BC

<https://docs.paloaltonetworks.com/sd-wan/3-0/sd-wan-admin/configure-sd-wan/create-full-mesh-vpn-cluster-with-ddns>

upvoted 2 times

—  **Alvin1987** 3 years, 7 months ago

<https://docs.paloaltonetworks.com/plugins/vm-series-and-panorama-plugins-release-notes/panorama-plugin-for-sd-wan/sd-wan-plugin-200/features-introduced-in-sd-wan-2-0.html>

B&C - With 2.0.2 sd-wan plugin it supports full-mesh in addition to hub and spoke type

upvoted 2 times

—  **Alvin1987** 3 years, 7 months ago

<https://docs.paloaltonetworks.com/plugins/vm-series-and-panorama-plugins-release-notes/panorama-plugin-for-sd-wan/sd-wan-plugin-200/features-introduced-in-sd-wan-2-0.html>


With 2.0.2 plugin it supports full-mesh in addition to hub&spoke. So, the answer should be B&C

upvoted 1 times

—  **Mr_Cipher** 3 years, 8 months ago

B & C are the most accurate answers, as per this doco <https://www.paloguard.com/datasheets/sd-wan.pdf> --> "Palo Alto Networks supports multiple SD-WAN deployment options, including mesh, hub-and-spoke, and cloud-based deployments."

upvoted 2 times

—  **GBD** 3 years, 12 months ago

I think the real question about this question is this referring to SD-Wan in general or PAN's version of it?

upvoted 1 times

—  **alexblue** 4 years, 1 month ago

BC

The CloudGenix SD-WAN supports both hub-and-spoke and limited scale full-mesh designs managed through a cloud-based portal.

https://www.paloaltonetworks.nl/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/guides/pan-os-secure-sd-wan-deployment-guide

upvoted 3 times

—  **rammsdoct** 4 years, 2 months ago

it is very tricky question, seems like PA does not support full-mesh and only support Hub&spoke topology, however I would say that or either question is wrong or we can consider going VPN clustering as full-mesh (logically) if not, just hub and spoke, C

this doc said that full mesh is not supported:

<https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/configure-sd-wan/create-a-vpn-cluster.html>

and this said that p2p is supported

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-release-notes/pan-os-9-1-release-information/features-introduced-in-pan-os-9-1/sd-wan-features>

so I will go A and C

upvoted 1 times

  **rammsdoct** 4 years, 2 months ago

woops correct myself A-B p2p and Hub&spoke

upvoted 1 times

  **yashishinde** 4 years, 2 months ago

Correct ans: BC

<http://www.paloguard.com/datasheets/sd-wan.pdf>

upvoted 1 times

  **ChiaPet75** 4 years, 2 months ago

I guess you are correct yashishinde it says Mesh is supported, or it will be supported soon. There is some conflict between the current documentation and the datasheet.

upvoted 1 times

  **ChiaPet75** 4 years, 2 months ago

Correct: A,C

Hub-and-Spoke is the default topology for PaloAlto SD-WAN

Auto VPN Topology Creation - VPN clusters simplify the creation of complex VPN topologies using logical groupings of branches and hubs to accelerate the configuration and deployment of secure communications between all locations. (I guess this could be considered full-mesh but only in the logical sense.)

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-release-notes/pan-os-9-1-release-information/features-introduced-in-pan-os-9-1/sd-wan-features>

Full mesh is not supported in PAN-OS version 9.1.0

<https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/configure-sd-wan/create-a-vpn-cluster.html>

upvoted 1 times

  **santino** 4 years, 3 months ago

I think it is A and B

Full Mesh SD-WAN VPN topology is not supported in PAN-OS 9.1.0.

<https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/configure-sd-wan/create-a-vpn-cluster.html>

upvoted 3 times

  **mmaasa** 4 years, 2 months ago

Its actually only support Hub-Spoke. The question should be asking for only 1 answer instead of 2. Based on the document you provided, "Only Hub-Spoke VPN cluster type is supported in PAN-OS 9.1.0."

upvoted 1 times

  **zadkiel** 4 years, 1 month ago

peer to peer is basically hub-spoke with only one peer. If you can't connect to a single peer you can't form hub-spoke. IMHO

upvoted 1 times

Which option describes the operation of the automatic commit recovery feature?

- A. It enables a firewall to revert to the previous configuration if rule shadowing is detected.
- B. It enables a firewall to revert to the previous configuration if application dependency errors are found.
- C. It enables a firewall to revert to the previous configuration if a commit causes HA partner connectivity failure.
- D. It enables a firewall to revert to the previous configuration if a commit causes Panorama connectivity failure.

Correct Answer: D

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/panorama-features/automatic-panorama-connection-recovery.html>

Daniel2020 Highly Voted 3 years, 10 months ago

D

It was a feature released since 9.1 with a slightly different name.

PAN-OS 10.0 <https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/administer-panorama/enable-automated-commit-recovery.html>

PAN-OS 9.1 <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/panorama-features/automatic-panorama-connection-recovery.html>
upvoted 5 times

scanossa Most Recent 7 months ago

Selected Answer: D

After checking on our lab we confirmed that as soon as a new config breaks communication between Panorama and one of the FWs, it reverts to the previous config.

upvoted 1 times

Marshpillowz 7 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

lol12 1 year, 10 months ago

Selected Answer: D

D

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/administer-panorama/enable-automated-commit-recovery.html>
upvoted 2 times

TAKUM1y 1 year, 10 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/administer-panorama/enable-automated-commit-recovery.html>
upvoted 2 times

UFanat 2 years, 2 months ago

Selected Answer: D

Panorama connectivity failure leads to reverting config

upvoted 1 times

NLT 2 years, 6 months ago

To ensure that broken configurations caused by configuration changes pushed from the Panorama™ management server to managed firewalls, or committed locally on the firewall, enable Automated Commit Recovery to enable managed firewalls to test configuration changes for each commit and to verify that the changes did not break the connection between Panorama and the managed firewall.

upvoted 1 times

gaplayer26 2 years, 10 months ago

It's D - all the answers are related to..." firewall to revert..." and the link in the answer refers to 'Connection Recovery' not, -> Firewall Commit Recovery...

Process of elimination here.

upvoted 1 times

mmed 3 years, 5 months ago

D

<https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/administer-panorama/enable-automated-commit-recovery.html>
upvoted 3 times

Which three items are important considerations during SD-WAN configuration planning? (Choose three.)

- A. branch and hub locations
- B. link requirements
- C. the name of the ISP
- D. IP Addresses

Correct Answer: ABD

Reference:

<https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/plan-sd-wan-configuration>

  **Plato22** Highly Voted 2 years, 8 months ago



To me, I would stay away from Century Link, so C is important to me...lol
But they are looking for A, B and D.

upvoted 10 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: ABD

A, B and D correct
upvoted 1 times

  **lol12** 1 year, 10 months ago

Selected Answer: ABD

ABD
<https://docs.paloaltonetworks.com/sd-wan/3-0/sd-wan-admin/sd-wan-overview/plan-sd-wan-configuration>
upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago


Selected Answer: ABD

<https://docs.paloaltonetworks.com/sd-wan/3-0/sd-wan-admin/sd-wan-overview/plan-sd-wan-configuration>
upvoted 1 times



  **UFanat** 2 years, 2 months ago

Selected Answer: ABD

ABD. It does not matter what is the name of the ISP
upvoted 1 times

  **Prutser2** 3 years, 2 months ago



common sense question, so a b d
upvoted 2 times

  **Pag0s** 3 years, 6 months ago

ABD is the correct answer
upvoted 4 times

  **B2020Nov** 3 years, 9 months ago

<https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/plan-sd-wan-configuration>
upvoted 2 times

  **Mr_Cipher** 3 years, 8 months ago

Obviously, ISP name is irrelevant whatsoever :)
upvoted 5 times

Starting with PAN-OS version 9.1, application dependency information is now reported in which two locations? (Choose two.)

- A. on the App Dependency tab in the Commit Status window
- B. on the Policy Optimizer's Rule Usage page
- C. on the Application tab in the Security Policy Rule creation window
- D. on the Objects > Applications browser pages

Correct Answer: AC

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/use-application-objects-in-policy/resolve-application-dependencies>


  **hcir** 2 months, 2 weeks ago

Dependencies can be seen in objects --> Applications, but the question specifically asks "starting with 9.1" which are A and C
upvoted 1 times

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: AC

A and C correct
upvoted 1 times

  **lol12** 1 year, 10 months ago



Selected Answer: AC

AC
<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/use-application-objects-in-policy/resolve-application-dependencies>
upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: AC

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/use-application-objects-in-policy/resolve-application-dependencies>
upvoted 1 times

  **jshow** 2 years, 2 months ago

A-C Pg 175
upvoted 2 times


  **tenebrox** 2 years, 2 months ago

Selected Answer: AC

D its not possible "D. on the Objects > Applications browser pages", you can see the depends it by clicking on the application not in the app browser
upvoted 3 times

  **randomtotiti** 2 years, 3 months ago

D is also right, you can check which apps an app depends on in the application details
upvoted 1 times

  **Elvenking** 2 years, 4 months ago

Selected Answer: AC

Doc for PanOS v10.1:
<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/app-id/use-application-objects-in-policy/resolve-application-dependencies>
upvoted 3 times

  **poiuytr** 2 years, 4 months ago

so answers are = A,C
upvoted 1 times

Which two events trigger the operation of automatic commit recovery? (Choose two.)

- A. when an aggregate Ethernet interface component fails
- B. when Panorama pushes a configuration
- C. when a firewall performs a local commit
- D. when a firewall HA pair fails over



Correct Answer: BC

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/panorama-features/automatic-panorama-connection-recovery.html>

  **ThomasDao** Highly Voted 3 years, 6 months ago

yes B, C ... pcnse study guide - page 284
upvoted 6 times

  **mic_mic** Highly Voted 1 year, 7 months ago

Selected Answer: BC

Bad question, it must be: "Which two events CAN trigger the operation of automatic commit recovery? (Choose two.)"
upvoted 5 times

  **Od2fdfa** Most Recent 3 months, 3 weeks ago

Selected Answer: BC

auto commit is to make sure firewall does not loose connectivity to panorama.
upvoted 1 times

  **hcir** 2 months, 2 weeks ago

it is not auto commit but auto commit recovery. These are 2 different things
upvoted 1 times

  **scanossa** 7 months ago

Selected Answer: BC

These 2 actions might break FW-Panorama communication
upvoted 2 times

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: BC

B and C correct
upvoted 1 times

  **GohanF2** 1 year, 6 months ago


BC.
STUDY GUIDE 2023. PAGE 172.
upvoted 3 times

  **lol12** 1 year, 10 months ago

Selected Answer: BC



BC
<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/administer-panorama/enable-automated-commit-recovery>

Wouldn't make sense if we had commit recovery every time an interface went down
upvoted 3 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: BC

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/administer-panorama/enable-automated-commit-recovery>
upvoted 2 times

  **NLT** 2 years, 6 months ago

Automatic commit recovery allows you to configure the firewall to attempt a specified number of connectivity tests after you push a configuration from Panorama or commit a configuration change locally on the firewall.
upvoted 3 times

  **B2020Nov** 3 years, 9 months ago

Yes B, C

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/panorama-features/automatic-panorama-connection-recovery.html>
upvoted 5 times

 **MyWil** 4 years ago

Automatic commit recovery allows you to configure the firewall to attempt a specified number of connectivity tests after:

- 1- you push a configuration from Panorama or
- 2- commit a configuration change locally on the firewall.

Additionally, the firewall checks connectivity to Panorama every hour to ensure consistent communication in the event unrelated network configuration changes have disrupted connectivity between the firewall and Panorama or if implications to a pushed committed configuration may have affected connectivity.

upvoted 3 times

Panorama provides which two SD-WAN functions? (Choose two.)

- A. network monitoring
- B. control plane
- C. data plane
- D. physical network links

Correct Answer: AB

dman7 Highly Voted 4 years, 3 months ago

I think it is A & B
upvoted 19 times

Ab121213 4 years, 3 months ago

C and D are irrelevant
upvoted 5 times

jpm_1506 3 years, 8 months ago

agreed. panorama wont be involved in the data plane, and has nothing to do with physical links. however it will provide monitoring and control plane so must be AB
upvoted 1 times

sethjam Highly Voted 4 years, 2 months ago

The question is Panorama which provides management (control plane) and also provide visibility (network monitoring). Answer for me is A&B.
upvoted 10 times

scanossa Most Recent 7 months ago

Selected Answer: AB

C and D are related to firewalls
upvoted 1 times

Marshpillowz 7 months, 1 week ago

Selected Answer: AB

A and B correct
upvoted 1 times

TAKUM1y 1 year, 10 months ago

Selected Answer: AB

<https://docs.paloaltonetworks.com/sd-wan/3-0/sd-wan-admin/sd-wan-overview/about-sd-wan>
upvoted 3 times

UFanat 2 years, 2 months ago

Selected Answer: AB

Panorama does not have data plane, but it acts as a control plane with network monitoring capabilities.
upvoted 2 times

yapj 2 years, 3 months ago

Selected Answer: AB

control only
upvoted 3 times

Breyarg 2 years, 8 months ago

we have this in production. its AB. you need panorama for the control of the SDWAN and also to allow monitoring of the network once in SDWAN mode.
upvoted 1 times

achille5 3 years, 4 months ago

A & B
<https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/about-sd-wan.html>
upvoted 1 times

VivekSL512 3 years, 5 months ago

A & B (Network Monitoring & Control Plane). Data plane & Physical Interfaces are directly taken care through Firewalls where SD WAN is enabled.
upvoted 1 times

[-] 👤 **ThomasDao** 3 years, 6 months ago

Yes A, B ... sd-wan admin page 9

upvoted 2 times

[-] 👤 **Helloory** 4 years ago

Correct answer is A & B

<https://www.paloaltonetworks.com/resources/guides/sd-wan-architecture-guide>

The PAN-OS Secure SD-WAN solution is orchestrated by Panorama™, which you use to configure and monitor the central-site and remote-site devices.

upvoted 3 times

[-] 👤 **alpha520** 4 years, 2 months ago

A&B are correct

upvoted 4 times

[-] 👤 **rammsdoct** 4 years, 2 months ago

Actually can be ABC

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-release-notes/pan-os-9-1-release-information/features-introduced-in-pan-os-9-1/sd-wan-features>

but I guess that BC for me

upvoted 1 times

[-] 👤 **ChiaPet75** 4 years, 2 months ago

Answers: B,C

How Does SD-WAN Work?

Traditional WANs rely on physical routers to connect remote or branch users to applications hosted on data centers. Each router has a [data plane], which holds the information, and a [control plane], which tells the data where to go. Where data flows is typically determined by a network engineer or administrator who writes rules and policies, often manually, for each router on the network – a process that can be time-consuming and prone to errors.

SD-WAN separates the control and management processes from the underlying networking hardware, making them available as software that can be easily configured and deployed. A centralized control pane means network administrators can write new rules and policies, and then configure and deploy them across an entire network at once.

<https://www.paloaltonetworks.com/cyberpedia/what-is-a-sd-wan>

upvoted 2 times

Updates to dynamic user group membership are automatic therefore using dynamic user groups instead of static group objects allows you to:

- A. respond to changes in user behaviour or potential threats using manual policy changes
- B. respond to changes in user behaviour or potential threats without manual policy changes
- C. respond to changes in user behaviour or potential threats without automatic policy changes
- D. respond to changes in user behaviour and confirmed threats with manual policy changes

Correct Answer: B

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/use-dynamic-user-groups-in-policy.html>



  **Prutser2** Highly Voted 3 years, 2 months ago

common sense question, B
upvoted 6 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: B

B is correct
upvoted 1 times

  **lol12** 1 year, 10 months ago



Selected Answer: B

B
Common sense
upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: B

B is a correct answer
upvoted 2 times

  **mmed** 3 years, 5 months ago

CORRECT B
<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups>
upvoted 3 times















How can an administrator configure the firewall to automatically quarantine a device using GlobalProtect?





- A. by adding the device's Host ID to a quarantine list and configure GlobalProtect to prevent users from connecting to the GlobalProtect gateway from a quarantined device
- B. by exporting the list of quarantined devices to a pdf or csv file by selecting PDF/CSV at the bottom of the Device Quarantine page and leveraging the appropriate XSOAR playbook
- C. by using security policies, log forwarding profiles, and log settings
- D. there is no native auto-quarantine feature so a custom script would need to be leveraged

Correct Answer: C

Reference:

<https://docs.paloaltonetworks.com/globalprotect/10-0/globalprotect-admin/host-information/quarantine-devices-using-host-information/automatically-quarantine-a-device>

-   **mmed** Highly Voted 3 years, 5 months ago
confirm c
<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/globalprotect-features/identification-and-quarantine-of-compromised-devices.html>
upvoted 7 times
-   **Marshpillowz** Most Recent 7 months, 1 week ago
Selected Answer: C
C is correct
upvoted 1 times
-   **lol12** 1 year, 10 months ago
Selected Answer: C
C
<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/host-information/quarantine-devices-using-host-information/automatically-quarantine-a-device>
upvoted 3 times
-   **NLT** 2 years, 6 months ago
After you identify a device as compromised (for example, if a device has been infected with malware and is performing command and control actions), you can manually add the device's Host ID to a quarantine list and configure GlobalProtect to prevent users from connecting to the GlobalProtect gateway from a quarantined device. You can also automatically quarantine the device using security policies, log forwarding profiles, and log settings.
upvoted 4 times
-   **Gilmarcio** 2 years, 7 months ago
Correct "C"
<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/host-information/quarantine-devices-using-host-information/automatically-quarantine-a-device.html#idb42b2b82-b253-4be7-9840-1efa49dba3da>
upvoted 1 times
-   **Plato22** 2 years, 8 months ago
Answer is C. Read the wording of the question and then find the answer here:
<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/globalprotect-features/identification-and-quarantine-of-compromised-devices.html>
upvoted 3 times
-   **prosto_marussia** 2 years, 9 months ago
After you identify a device as compromised (for example, if a device has been infected with malware and is performing command and control actions), you can manually add the device's Host ID to a quarantine list and configure GlobalProtect to prevent users from connecting to the GlobalProtect gateway from a quarantined device. You can also automatically quarantine the device using security policies, log forwarding profiles, and log settings.

Both A and C kinda work.
upvoted 1 times
-   **Martian89** 2 years, 1 month ago
A is not automatic though (question is about automatic quarantine)
upvoted 2 times
-   **Biz90** 2 years, 10 months ago

Hi Team, the answer is A based on the KB below it even tells you that:

'you can manually add the device's Host ID to a quarantine list and configure GlobalProtect to prevent users from connecting to the GlobalProtect gateway from a quarantined device'

upvoted 1 times

  **Breyarg** 2 years, 8 months ago

i agree but then re-read the question it implies "automatically" which suggests no manual intervention. so only "C" can be correct now.

upvoted 3 times

Question #165

Topic 1

To protect your firewall and network from single source denial of service (DoS) attacks that can overwhelm its packet buffer and cause legitimate traffic to drop, you can configure:

- A. PBP (Protocol Based Protection)
- B. BGP (Border Gateway Protocol)
- C. PGP (Packet Gateway Protocol)
- D. PBP (Packet Buffer Protection)

Correct Answer: D

Reference:



<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/packet-buffer-protection>

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

  **lol12** 1 year, 10 months ago

Selected Answer: D

D

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/packet-buffer-protection>

Packet Buffer Protection defends your firewall and network from single session DoS attacks that can overwhelm the firewall's packet buffer and cause legitimate traffic to drop. Although you don't configure Packet Buffer Protection in a Zone Protection profile or in a DoS Protection profile or policy rule, Packet Buffer Protection defends ingress zones. While zone and DoS protection apply to new sessions (connections) and are granular, Packet Buffer Protection applies to existing sessions and is global.

upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: D

Packet Buffer Protection (part of Zone Protection)

upvoted 2 times

  **Gilmarcio** 2 years, 7 months ago



Correct "D" - <https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/packet-buffer-protection.html>

upvoted 3 times

  **rubberbudgie** 3 years, 3 months ago

Correct D - <https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/packet-buffer-protection.html>

upvoted 4 times

  **pajonk** 3 years, 5 months ago

Correct D

upvoted 4 times

A bootstrap USB flash drive has been prepared using a Windows workstation to load the initial configuration of a firewall that was previously being used in a lab.

The USB flash drive was formatted using file system FAT32 and the initial configuration is stored in a file named init-cfg.txt. The firewall is currently running PAN-



OS 10.0 and using a lab config. The contents of init-cfg.txt in the USB flash drive are as follows:

```
type=dhcp-client
ip-address=
default-gateway=
netmask=
ipv6-address=
ipv6-default-gateway=
hostname=Ca-FW-DC1
panorama-server=10.5.107.20
panorama-server-2=10.5.107.21
tplname=FINANCE_TG4
dgname=finance_dg
dns-primary=10.5.6.6
dns-secondary=10.5.6.7
op-command-modes=multi-vsyst,jumbo-frame
dhcp-send-hostname=yes
dhcp-send-client-id=yes
dhcp-accept-server-hostname=yes
dhcp-accept-server-domain=yes
```

The USB flash drive has been inserted in the firewalls' USB port, and the firewall has been restarted using command: > request restart system
Upon restart, the firewall fails to begin the bootstrapping process. The failure is caused because:

- A. The bootstrap.xml file is a required file, but it is missing
- B. Firewall must be in factory default state or have all private data deleted for bootstrapping
- C. The hostname is a required parameter, but it is missing in init-cfg.txt
- D. The USB must be formatted using the ext3 file system. FAT32 is not supported

Correct Answer: D



  **hpbdc** Highly Voted 1 year, 11 months ago

Selected Answer: B

absolutely B:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/bootstrap-the-firewall/bootstrap-a-firewall-using-a-usb-flash-drive>

upvoted 9 times

  **Woody** 1 year, 8 months ago

Agreed B.

upvoted 2 times

  **news088** Highly Voted 1 year, 7 months ago

Fat 32 is supported . So D is not correct

The correct response is B

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/firewall-administration/bootstrap-the-firewall/usb-flash-drive-support>

upvoted 6 times

  **afrozkhano9** Most Recent 1 day, 5 hours ago


Answer: B

upvoted 1 times

  **BhushanW** 1 day, 21 hours ago

D: Microsoft Windows and Apple Mac operating systems are unable to read the bootstrap USB flash drive because the drive is formatted using an ext4 file system. You must install third-party software or use a Linux system to read the USB drive.

upvoted 1 times

  **dtisolutions** 6 months, 1 week ago

Selected Answer: B


B is the correct answer for sure

upvoted 1 times

[-]  **Marshpillowz** 7 months, 1 week ago


Selected Answer: B

B is correct
upvoted 1 times

[-]  **Yetti254** 7 months, 3 weeks ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/bootstrap-the-firewall/bootstrap-a-firewall-using-a-usb-flash-drive>
upvoted 1 times


[-]  **JRKhan** 7 months, 3 weeks ago

Selected Answer: B

B is correct.
upvoted 1 times

[-]  **yaboi01** 1 year, 1 month ago

Answer is B:
PCNSE Study Guide Pg 86 section2.4.4
upvoted 1 times


[-]  **Techn** 1 year, 2 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/bootstrap-the-firewall/bootstrap-a-firewall-using-a-usb-flash-drive>
upvoted 1 times

[-]  **Pochex** 1 year, 6 months ago

B is the correct =====> For security reasons, you can bootstrap a firewall only when it is in factory default state or has all private data deleted.
upvoted 1 times

[-]  **DenskyDen** 1 year, 7 months ago


Selected Answer: B

The firewall must be in a factory default state or must have all private data deleted.
upvoted 1 times

[-]  **bearfromdownunder** 1 year, 7 months ago

Selected Answer: B


Firewall should be in factory default
upvoted 1 times

[-]  **lol12** 1 year, 10 months ago

Selected Answer: B

B

The firewall must be in a factory default state or must have all private data deleted.
upvoted 3 times

[-]  **spydog** 1 year, 11 months ago

Selected Answer: B

Firewall must be in factory default state for the bootstrap process to be triggered
upvoted 2 times

[-]  **mizuno92** 1 year, 11 months ago

Selected Answer: B

Firewall must start in factory default state. Page 105 study guide.
upvoted 1 times

[-]  **melmokad** 1 year, 11 months ago

bootstrap.xml is optional
upvoted 1 times

An Administrator is configuring Authentication Enforcement and they would like to create an exemption rule to exempt a specific group from authentication. Which authentication enforcement object should they select?

- A. default-no-captive-portal
- B. default-authentication-bypass
- C. default-browser-challenge
- D. default-web-form

Correct Answer: A

Reference:


<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-authentication>

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

  **aatechler** 1 year, 7 months ago

Selected Answer: A

default-browser-challenge—The firewall transparently obtains user authentication credentials

default-web-form—To authenticate users, the firewall uses the certificate profile or authentication profile you specified when configuring Authentication Portal

default-no-captive-portal—The firewall evaluates Security policy without authenticating users.

upvoted 2 times

  **lol12** 1 year, 10 months ago

Selected Answer: A

A

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/objects/objects-authentication>



upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: A

no captive portal - is a correct option to bypass auth rules

upvoted 2 times

  **NLT** 2 years, 6 months ago

default-no-captive-portal—The firewall evaluates Security policy without authenticating users.

upvoted 3 times

  **rubberbudgie** 3 years, 3 months ago

Correct A - <https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-web-interface-help/objects/objects-authentication.html>

upvoted 2 times

  **VivekSL512** 3 years, 5 months ago

Correct: A

upvoted 4 times

A bootstrap USB flash drive has been prepared using a Linux workstation to load the initial configuration of a Palo Alto Networks firewall. The USB flash drive was formatted using file system ntfs and the initial configuration is stored in a file named init-cfg.txt.

The contents of init-cfg.txt in the USB flash drive are as follows:

```
type=static
ip-address=10.5.107.19
default-gateway=10.5.107.1
netmask=255.255.255.0
ipv6-address=2001:400:f00::1/64
ipv6-default-gateway=2001:400:f00::2
hostname=Ca-FW-DC1
panorama-server=10.5.107.20
panorama-server-2=10.5.107.21
tplname=FINANCE_TG4
dgname=finance_dg
dns_primary=10.5.6.6
dns-secondary=10.5.6.7
op-command-modes=multi-vsyst, jumbo-frame
dhcp-send-hostname=no
dhcp-send-client-id=no
dhcp-accept-server-hostname=no
dhcp-accept-server-domain=no
```

The USB flash drive has been inserted in the firewalls' USB port, and the firewall has been powered on. Upon boot, the firewall fails to begin the bootstrapping process. The failure is caused because:

- A. the bootstrap.xml file is a required file, but it is missing
- B. nit-cfg.txt is an incorrect filename, the correct filename should be init-cfg.xml
- C. The USB must be formatted using the ext4 file system
- D. There must be commas between the parameter names and their values instead of the equal symbols
- E. The USB drive has been formatted with an unsupported file system

Correct Answer: E



  **Blut** Highly Voted 3 years, 5 months ago

As per PA it will support FAT32 and ext3 so the correct ans is E (Unsupported File System)

The USB flash drive that bootstraps a hardware-based Palo Alto Networks firewall must support one of the following:

- File Allocation Table 32 (FAT32)
- Third Extended File System (ext3)

upvoted 11 times

  **Trung2735** 3 years ago

The link <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/firewall-administration/bootstrap-the-firewall/usb-flash-drive-support.html>

upvoted 3 times

  **VivekSL512** Highly Voted 3 years, 5 months ago

Correct answer is E - Unsupported File System



upvoted 6 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: E


E is correct

upvoted 1 times

  **Narbo** 1 year, 6 months ago

The question states that the USB was already formatted using ntfs, which is unsupported. E is correct.

upvoted 1 times

  **MrR0bot** 1 year, 7 months ago

Selected Answer: E



E is correct

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/firewall-administration/bootstrap-the-firewall/usb-flash-drive-support>
The USB flash drive that bootstraps a hardware-based Palo Alto Networks firewall must support one of the following:

File Allocation Table 32 (FAT32)

Third Extended File System (ext3)

upvoted 2 times

  **javim** 1 year, 7 months ago

Selected Answer: C

The correct answer is C.

For bootstrapping the USB must be in ext4 format

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/bootstrap-the-firewall/bootstrap-a-firewall-using-a-usb-flash-drive>

upvoted 1 times

  **secdaddy** 1 year, 11 months ago

Because all Linux users always use NTFS :-D

upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: E

File name should be init-cfg.txt (not xml) (B is incorrect)

Config looks fine according to:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/bootstrap-the-firewall/sample-init-cfgtxt-files> (D is not correct)

option A - looks stupid

Supported file systems ext3 and FAT32, so it should be E

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/bootstrap-the-firewall/usb-flash-drive-support>

upvoted 3 times

  **Gilmarcio** 2 years, 7 months ago

Correct "E" File system is ext3 or fat32

upvoted 2 times

  **homersimpson** 2 years, 8 months ago

Selected Answer: E

Filesystems supported are ext3, fat32

upvoted 3 times

  **Plato22** 2 years, 8 months ago

Should be E

upvoted 1 times

  **lucaboban** 3 years, 5 months ago

Correct answer is C

USB flash drive should be formatted using an ext4 file system

upvoted 3 times

  **VivekSL512** 3 years, 5 months ago

Sorry.. C is not correct answer - Supported File Systems are - FAT32 and Ext3. Please refer below admin guide and you can search with keyword "FAT32" and you will get your answer.

https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/8-1/pan-os-admin/pan-os-admin.pdf

upvoted 2 times

  **VivekSL512** 3 years, 5 months ago

Correct Answer is E - Unsupported File System

upvoted 3 times



  **ggWillis** 3 years, 1 month ago

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/firewall-administration/bootstrap-the-firewall/bootstrap-a-firewall-using-a-usb-flash-drive.html>

Wrong, ext4 is the only supported file system

correct answer is C

upvoted 2 times

  **Trung2735** 3 years ago

"Microsoft Windows and Apple Mac operating systems are unable to read the bootstrap USB flash drive because the drive is formatted using an ext4 file system. You must install third-party software or use a Linux system to read the USB drive."

This is them confusing people. It only state that Windows and Mac are unable to read the USB.

upvoted 1 times

  **GivemeMoney** 2 years, 7 months ago

Wrong FAT32 and EXT3 are supported, so the answer is D.



[s/10-1/pan-os-admin/firewall-administration/bootstrap-the-firewall/usb-flash-drive-support.html](https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/firewall-administration/bootstrap-the-firewall/usb-flash-drive-support.html)

upvoted 1 times

  **GivemeMoney** 2 years, 7 months ago

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/firewall-administration/bootstrap-the-firewall/usb-flash-drive-support.html>

upvoted 1 times

  **javim** 1 year, 7 months ago

It's correct. The answer is C.

For bootstrapping the USB must be in ext4 format

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/bootstrap-the-firewall/bootstrap-a-firewall-using-a-usb-flash-drive>

upvoted 1 times

Question #169

Topic 1

To more easily reuse templates and template stacks, you can create template variables in place of firewall-specific and appliance-specific IP literals in your configurations.

Which one is the correct configuration?

A. &Panorama

B. @Panorama

C. \$Panorama

D. #Panorama

Correct Answer: C

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-new-features/panorama-features/configuration-reusability-for-templates-and-template-stacks.html>

  **scanossa** 7 months ago

Selected Answer: C

\$, confirmed from Panorama


upvoted 1 times

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: C



\$ should be used

upvoted 2 times

  **Gilmarcio** 2 years, 7 months ago

correct "C" - Templates variable - "\$"Panorama

upvoted 3 times

  **mmed** 3 years, 5 months ago

confirm C

Create a template and template stack using a variable name for an object. Variable names must start with the dollar sign ("\$") symbol. For example, you could use \$Panorama as a variable for the Panorama IP address that you want to configure on multiple managed firewalls and appliances

upvoted 4 times

  **VivekSL512** 3 years, 5 months ago

Correct: C

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-new-features/panorama-features/configuration-reusability-for-templates-and-template-stacks.html>

upvoted 4 times

On the NGFW, how can you generate and block a private key from export and thus harden your security posture and prevent rogue administrators or other bad actors from misusing keys?

- A. 1. Select Device > Certificate Management > Certificates > Device > Certificates 2. Import the certificate 3. Select Import Private key 4. Click Generate to generate the new certificate
- B. 1. Select Device > Certificates 2. Select Certificate Profile 3. Generate the certificate 4. Select Block Private Key Export
- C. 1. Select Device > Certificate Management > Certificates > Device > Certificates 2. Generate the certificate 3. Select Block Private Key Export 4. Click Generate to generate the new certificate
- D. 1. Select Device > Certificates 2. Select Certificate Profile 3. Generate the certificate 4. Select Block Private Key Export

Correct Answer: C

Reference:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/decryption-features/block-export-of-private-keys.html>

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

  **lol12** 1 year, 10 months ago

Selected Answer: C

C

Available answers have typos and it should be

Select Device > Certificate Management > Certificates > Device Certificates

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/block-private-key-export/generate-a-private-key-and-block-it>

upvoted 4 times

  **Pretorian** 2 years ago

Messed up/redundant path but, the only possible answer is C

upvoted 1 times

  **Gilmarcio** 2 years, 7 months ago

Correct "C"

1 - <https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/decryption-features/block-export-of-private-keys.html>

2 - <https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/block-private-key-export>

upvoted 2 times

  **khurshid** 2 years, 7 months ago



C is correct

upvoted 2 times

  **rubberbudgie** 3 years, 3 months ago



Correct C - <https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/decryption-features/block-export-of-private-keys.html>

upvoted 4 times

  **mmed** 3 years, 5 months ago

confirm c

upvoted 1 times

  **lucaboban** 3 years, 5 months ago

C is correct

upvoted 1 times

What is the maximum number of samples that can be submitted to WildFire manually per day?

- A. 1,000
- B. 2,000
- C. 5,000
- D. 15,000

Correct Answer: A

Reference:

<https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/submit-files-for-wildfire-analysis/manually-upload-files-to-the-wildfire-portal.html#:~:text=If%20you%20have%20a%20WildFire,also%20includes%20WildFire%20API%20submissions>

mmed Highly Voted 3 years, 5 months ago

confrim A
1000 submission
10,000 query
upvoted 9 times

duckduckgoo 1 year, 5 months ago

Yup, that got me. THanks
upvoted 2 times

hcir Most Recent 2 months, 1 week ago

actually, they changed the values. It is now 2,500 daily submissions and 17,500 queries peri API SKU (including manual submissions), but for some reason, they did not update techdoc. So if you see 2,500 in the exam, bear this in mind.
upvoted 3 times

Marshpillowz 7 months, 1 week ago

Selected Answer: A

Correct answer is A
upvoted 1 times

TAKUM1y 1 year, 10 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/submit-files-for-wildfire-analysis/manually-upload-files-to-the-wildfire-portal>
upvoted 2 times

UFanat 2 years, 2 months ago

Selected Answer: A

A
1000 file submission
and
10,000 queries
upvoted 3 times

rubberbudgie 3 years, 3 months ago

Correct A - <https://docs.paloaltonetworks.com/wildfire/10-0/wildfire-admin/submit-files-for-wildfire-analysis/manually-upload-files-to-the-wildfire-portal.html>
upvoted 2 times

What file type upload is supported as part of the basic WildFire service?

- A. ELF
- B. BAT
- C. PE
- D. VBS

Correct Answer: C

Reference:

<https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/wildfire-subscription.html#:~:text=With%20the%20basic%20WildFire%20service,available%20every%2024%2D48%20hours>

  **rubberbudgie** Highly Voted 3 years, 3 months ago

Correct C - <https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/wildfire-subscription.html>
upvoted 9 times

  **Marshpillowz** Most Recent 7 months, 1 week ago



Selected Answer: C

C is correct
upvoted 1 times

  **Knowledge33** 1 year, 2 months ago


Selected Answer: C

<https://docs.paloaltonetworks.com/advanced-wildfire/administration/advanced-wildfire-overview/advanced-wildfire-subscription#:~:text=With%20the%20basic%20WildFire%20service,available%20every%2024%2D48%20hours>
upvoted 1 times



  **Knowledge33** 1 year, 2 months ago

" File Type Support—In addition to PEs, forward advanced file types for Advanced WildFire analysis, including APKs, Flash files, PDFs, Microsoft Office files, Java Applets, Java files (.jar and .class), and HTTP/HTTPS email links contained in SMTP and POP3 email messages. (WildFire private cloud analysis does not support APK, Mac OS X, Linux (ELF), archive (RAR/7-Zip), and script (JS, BAT, VBS, Shell Script, PS1, and HTA) files) "

upvoted 1 times

  **Pochex** 1 year, 6 months ago

Answer C =====> With the basic WildFire service, you can enable the firewall to forward portable executable (PE) files. Refer to <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/getting-started/enable-basic-wildfire-forwarding>
upvoted 1 times

  **droide** 1 year, 6 months ago

Selected Answer: C

By elimination it should be C.

ELF, BAT and VBS are in the advanced file type support :

WildFire Advanced File Type Support—In addition to PEs, forward advanced file types for WildFire analysis, including APKs, Flash files, PDFs, Microsoft Office files, Java Applets, Java files (.jar and .class), and HTTP/HTTPS email links contained in SMTP and POP3 email messages. (WildFire private cloud analysis does not support APK, Mac OS X, Linux (ELF), archive (RAR/7-Zip), and script (JS, BAT, VBS, Shell Script, PS1, and HTA) files).

link : <https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/wildfire-subscription>
upvoted 1 times

  **certprep2021** 1 year, 6 months ago

Selected Answer: C

"the firewall can forward portable executable (PE) files for WildFire analysis"

<https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/wildfire-subscription>
upvoted 1 times

  **Joyryde** 1 year, 6 months ago

Selected Answer: A

refer to gully300 documentation
upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

C. With the basic WildFire service, the firewall can forward portable executable (PE) files for WildFire analysis,

upvoted 2 times

  **gully300** 1 year, 7 months ago

Selected Answer: A

the question refers to "Basic wildfire"



PE is listed under "Advanced file support" the one that isn't is ELF

<https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/wildfire-subscription>

--- WildFire Inline ML—(PAN-OS 10.0 and later) Prevent malicious variants of portable executables, executable and linked format (ELF) files, and PowerShell scripts....

--- WildFire Advanced File Type Support—....

upvoted 2 times

  **cempejon** 1 year, 6 months ago

From your URL -> With the basic WildFire service, the firewall can forward portable executable (PE) files for WildFire analysis



upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/wildfire-subscription>



upvoted 3 times

  **javim** 1 year, 7 months ago

It say the basic subscrition.

ELF is in advance subscription.

upvoted 2 times

  **pajonk** 3 years, 5 months ago

Correct C

upvoted 4 times

An administrator accidentally closed the commit window/screen before the commit was finished.

Which two options could the administrator use to verify the progress or success of that commit task? (Choose two.)

- A. Task Manager
- B. System Logs
- C. Traffic Logs
- D. Configuration Logs

Correct Answer: AB

Marshpillowz 7 months, 1 week ago

Selected Answer: AB

A and B correct
upvoted 1 times

DenskyDen 1 year, 7 months ago

AB. 100%
upvoted 1 times

TAKUM1y 1 year, 10 months ago

Selected Answer: AB

A: <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/web-interface-basics/task-manager>

B: <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-severity-levels/system-logs>
upvoted 2 times

UFanat 2 years, 2 months ago

Selected Answer: AB

You can see that Commit submitted in Configuration Logs, but if you want to check it - you should look at Systems Logs. It's General Event: Commit job succeeded. Completion time...
upvoted 1 times

fireb 2 years, 3 months ago

Correct answers: A & B
upvoted 1 times

Abu_Muhammad 2 years, 4 months ago

Selected Answer: AB

A&B
progress can't be identified by configuration logs.
upvoted 2 times

confusion 2 years, 5 months ago

Selected Answer: AB

AB is what I would select here.

Question says "progress or success".

The System log on one of my FWs says things like: "Commit job succeeded. Completion time = date time, JobID=number. User = username" and also "Commit job started processing. Dequeue time = date time. JobID=number. User = username", so this can show progress and/or success.

Task Manager is obviously correct and can show progress and/or success.

I would not go for D. Configuration Logs as there you can see success or fail and the exact config diff, but you can't find progress.
upvoted 3 times

Jared28 2 years, 6 months ago

Selected Answer: AB



AB confirmed in a live test. D, configuration log, simply has the Result as "submitted", the system log said "Commit job succeeded..."
upvoted 1 times

unknid 2 years, 7 months ago

Selected Answer: AD

It's A & D. If you check the system logging (e.g with "decription contains 'commit'", all you'll see is the autocommit completion, nothing else). Configuration logging shows commit succeeded successfully.

upvoted 1 times

  **UFanat** 2 years, 2 months ago

D is wrong. Configurations Logs shows only commit submission but not completion. For Completion you must go to System Logs
upvoted 3 times

  **bartbernini** 2 years, 7 months ago

Selected Answer: AB



The correct answer is A and B. I don't know if this information used to be contained within system logs, but they are no longer there; this information is only available within the task manager and configuration logs.

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-severity-levels/config-logs>
<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/web-interface-basics/task-manager.html>

upvoted 2 times

  **bartbernini** 2 years, 7 months ago

I meant AD
upvoted 1 times

  **UFanat** 2 years, 2 months ago



D is wrong. Configurations Logs shows only commit submission but not completion. For Completion you must go to System Logs. Just checked in my lab.
upvoted 1 times

  **Gilmarcio** 2 years, 7 months ago

Correct A & B - <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/panorama-web-interface/panorama-commit-operations.html>
upvoted 1 times

  **shinichi_88** 2 years, 7 months ago

A and D, 100%
upvoted 1 times

  **UFanat** 2 years, 2 months ago

D is wrong. Configurations Logs (D) shows only commit submission but not completion. For Completion you must go to System Logs (B). Just checked in my lab.
upvoted 1 times

Before an administrator of a VM-500 can enable DoS and zone protection, what actions need to be taken?

- A. Create a zone protection profile with flood protection configured to defend an entire egress zone against SYN, ICMP, ICMPv6, UDP, and other IP flood attacks.
- B. Add a WildFire subscription to activate DoS and zone protection features.
- C. Replace the hardware firewall, because DoS and zone protection are not available with VM-Series systems.
- D. Measure and monitor the CPU consumption of the firewall data plane to ensure that each firewall is properly sized to support DoS and zone protection.

Correct Answer: D

alanouaro Highly Voted 2 years, 8 months ago

Option D

Check and monitor firewall dataplane CPU consumption to ensure that each firewall is properly sized to support DoS and Zone Protection along with any other features that consume CPU cycles, such as decryption.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/zone-protection-and-dos-protection.html>

upvoted 7 times

Marshpillowz Most Recent 7 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

lol12 1 year, 10 months ago

Selected Answer: D

d

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection>

upvoted 3 times

TAKUM1y 1 year, 10 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection>

upvoted 2 times

UFanat 2 years, 2 months ago

Selected Answer: D

Check and monitor firewall dataplane CPU consumption to ensure that each firewall is properly sized to support DoS and Zone Protection along with any other features that consume CPU cycles, such as decryption. If you use Panorama to manage your firewalls, use Device Monitor (PanoramaManaged DevicesHealth) to check and monitor the CPU consumption of all managed firewalls at one time.

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection>

upvoted 1 times

fireb 2 years, 3 months ago

D is the correct option.

upvoted 1 times

Gilmarcio 2 years, 7 months ago

Correct is "D". Because not "entire egress zone". Ingress true.

1 - [https://docs.paloaltonetworks.com/best-practices/8-1/dos-and-zone-protection-best-practices/deploy-dos-and-zone-protection-using-best-practices.html#:~:text=DoS%20and%20Zone%20Protection%20help,device%20at%20the%20internet%20perimeter](https://docs.paloaltonetworks.com/best-practices/8-1/dos-and-zone-protection-best-practices/dos-and-zone-protection-best-practices/deploy-dos-and-zone-protection-using-best-practices.html#:~:text=DoS%20and%20Zone%20Protection%20help,device%20at%20the%20internet%20perimeter).

2 - <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense/take-baseline-cps-measurements-for-setting-flood-thresholds/how-to-measure-cps.html>

upvoted 3 times

rischa 2 years, 7 months ago

Option D is right


upvoted 2 times

Hiwanku 2 years, 8 months ago

Is D.

Check and monitor firewall dataplane CPU consumption to ensure that each firewall is properly sized to support DoS and Zone Protection along with any other features that consume CPU cycles, such as decryption. If you use Panorama to manage your firewalls, use Device Monitor (PanoramaManaged DevicesHealth) to check and monitor the CPU consumption of all managed firewalls at one time.

upvoted 4 times

 **Marcy** 2 years, 8 months ago

You are right. D.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/zone-protection-and-dos-protection.html>

upvoted 2 times

DRAG DROP -

Please match the terms to their corresponding definitions.

Select and Place:

Answer Area

management plane

signature matching

security processing

network processing

provides configuration, logging, and reporting separate processor, RAM, and hard drive

stream-based, uniform signature matching in exploits (IPS), virus, spyware, CC#, and SSN

high-density parallel processing for flexible standardized complex functions

network processing hardware-accelerated per-packet route lookup, MAC lookup, and NAT

Correct Answer:

Answer Area

management plane

signature matching

security processing

network processing

provides configuration, logging, and reporting separate processor, RAM, and hard drive

stream-based, uniform signature matching in exploits (IPS), virus, spyware, CC#, and SSN

high-density parallel processing for flexible standardized complex functions

network processing hardware-accelerated per-packet route lookup, MAC lookup, and NAT

Marshpillowz 7 months, 1 week ago

Answer is already in order
upvoted 2 times

Knowledge33 1 year, 2 months ago

already sorted
upvoted 1 times

poiuytr 2 years, 4 months ago

Left = Right

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcnse-study-guide.pdf

An organization has recently migrated its infrastructure and configuration to NGFWs, for which Panorama manages the devices. The organization is coming from a L2-L4 firewall vendor, but wants to use App-ID while identifying policies that are no longer needed. Which Panorama tool can help this organization?

- A. Test Policy Match
- B. Application Groups
- C. Policy Optimizer
- D. Config Audit

Correct Answer: C

  **Plato22** Highly Voted  2 years, 8 months ago

should be C:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/app-id-features/policy-optimizer.html>

upvoted 6 times

  **scanossa** Most Recent  7 months ago

Selected Answer: C

C is correct

upvoted 1 times

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/security-policy-rule-optimization>

upvoted 3 times

  **UFanat** 2 years, 2 months ago

Selected Answer: C

You don't have to upgrade firewalls that Panorama (9.0 or higher) manages to use the Policy Optimizer capabilities. However, to use the Rule Usage capabilities (Monitor Policy Rule Usage), managed firewalls must run PAN-OS 8.1 or later.

upvoted 3 times

  **AbuHussain** 2 years, 5 months ago

Selected Answer: C

Should be C

upvoted 4 times

  **Alen** 2 years, 5 months ago

Selected Answer: C

answer is C

upvoted 3 times

  **Gilmarcio** 2 years, 7 months ago

Correct "C" - <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/app-id-features/policy-optimizer>

upvoted 2 times

  **alanouaro** 2 years, 8 months ago

Option C

This new feature identifies port-based rules so you can convert them to application-based rules that allow the traffic or add applications to existing rules without compromising application availability.

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/app-id-features/policy-optimizer.html>

upvoted 3 times

  **Marcy** 2 years, 8 months ago



Should be C

upvoted 4 times

An organization is building a Bootstrap Package to deploy Palo Alto Networks VM-Series firewalls into their AWS tenant. Which two statements are correct regarding the bootstrap package contents? (Choose two.)

- A. The bootstrap package is stored on an AFS share or a discrete container file bucket.
- B. The bootstrap.xml file allows for automated deployment of VM-Series firewalls with full network and policy configurations.
- C. The /config, /content and /software folders are mandatory while the /license and /plugin folders are optional.
- D. The init-cfg.txt and bootstrap.xml files are both optional configuration items for the /config folder.
- E. The directory structure must include a /config, /content, /software and /license folders.

Correct Answer: BE

  **Plato22** Highly Voted 2 years, 8 months ago

So many wrong answers on this site. Should be B and E:

<https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/bootstrap-the-vm-series-firewall/bootstrap-the-vm-series-firewall-in-aws.html>

upvoted 8 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

B and E correct

upvoted 1 times

  **Frightened_Acrobat** 1 year, 5 months ago

Should be D and E.

You can leave a folder empty, but you must have all the \config, \content, \license, and \software folders. Bootstrap.xml and ini-cfg.txt are both stored in /config. If \config can be empty that makes D an option. B seems unlikely as bootstrap.xml is not mentioned anywhere in the instructions to Bootstrap the VM-Series Firewall on AWS

<https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/bootstrap-the-vm-series-firewall/bootstrap-the-vm-series-firewall-in-aws>

upvoted 1 times

  **Frightened_Acrobat** 1 year, 1 month ago

Changing my answer to B and E because of this document <https://docs.paloaltonetworks.com/vm-series/10-2/vm-series-deployment/bootstrap-the-vm-series-firewall/bootstrap-configuration-files#id37d59976-16c6-4c75-af8a-61f46e690d65>

"The bootstrap package must include the basic configuration in config/init-cfg.txt"

Though optional, bootstrap.xml "contains a complete configuration for the firewall."

upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: BE

B: <https://docs.paloaltonetworks.com/vm-series/10-2/vm-series-deployment/bootstrap-the-vm-series-firewall/prepare-the-bootstrap-package#id5575318c-1de8-497a-960a-1d7417feefa6>

E: <https://docs.paloaltonetworks.com/vm-series/10-2/vm-series-deployment/bootstrap-the-vm-series-firewall/bootstrap-the-vm-series-firewall-in-aws>

upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: BE

You can leave a folder empty, but you must have

/config,

/license,

/software, and

/content folders

so E is must.

upvoted 1 times

  **AbuHussain** 2 years, 5 months ago

Selected Answer: BE

answer is B & E <https://www.examttopics.com/exams/palo-alto-networks/pcnse/view/#>



upvoted 2 times

  **Alen** 2 years, 5 months ago


Selected Answer: BE

answer is B & E

upvoted 2 times

  **Gilmarcio** 2 years, 7 months ago

Correct "B-E"
upvoted 1 times

  **Imla89** 2 years, 7 months ago

Selected Answer: BE

as per below
upvoted 2 times

  **Marcy** 2 years, 8 months ago

BE
<https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/bootstrap-the-vm-series-firewall/bootstrap-the-vm-series-firewall-in-aws.html>
upvoted 2 times

  **RJ45TP** 2 years, 8 months ago

Great thanks B and E
upvoted 2 times

Which Panorama objects restrict administrative access to specific device-groups?

- A. admin roles
- B. authentication profiles
- C. templates
- D. access domains

Correct Answer: D

Reference:

<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/panorama-overview/role-based-access-control/access-domains>

  **alanouaro** Highly Voted 2 years, 8 months ago

Option D

Access domains control administrative access to specific Device Groups and templates, and also control the ability to switch context to the web interface of managed firewalls.

<https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/panorama-overview/role-based-access-control/access-domains.html>

upvoted 7 times

  **scanossa** Most Recent 7 months ago

Selected Answer: D

Access domains



upvoted 2 times

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

  **lol12** 1 year, 10 months ago

Selected Answer: D

D

Links as below


upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/role-based-access-control/access-domains>

upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: D

to restrict access to device groups you should use access domains

upvoted 1 times

An engineer is planning an SSL decryption implementation.

Which of the following statements is a best practice for SSL decryption?

- A. Obtain an enterprise CA-signed certificate for the Forward Trust certificate.
- B. Use an enterprise CA-signed certificate for the Forward Untrust certificate.
- C. Use the same Forward Trust certificate on all firewalls in the network.
- D. Obtain a certificate from a publicly trusted root CA for the Forward Trust certificate.

Correct Answer: A

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/configure-ssl-forward-proxy>

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: A



A is correct

upvoted 1 times

  **Chiquitabandita** 7 months, 1 week ago

I agree it should be A, but why is C wrong? once you add it to the certificate profile, I would think admins would use it on all of their firewalls in their domain?

upvoted 1 times

  **Pacheco** 6 months, 3 weeks ago

There's a doc somewhere out there that states the best practice is something along the lines of "you could use the same enterprise or self-signed root CA cert for all firewalls, but definitely should use it to generate a specific intermediate CA for each firewall, because if you use the same ones for all of them and something happens and you need to change CAs for your forward trust cert, you're gonna have to change it in all firewalls. If you use an intermediate CA for each firewall, signed by the root CA and something happens on one of your firewalls, you just need to change the intermediate CA cert <<<for that firewall only>>>

upvoted 1 times

  **joquin0020** 11 months, 2 weeks ago

Selected Answer: B

I don't understand the answers, which is better, 'to Use' or 'to Obtain'? What a confusing question.

upvoted 2 times

  **DatITGuyTho1337** 8 months, 2 weeks ago

You obtain certificates to use them.

upvoted 1 times

  **lol12** 1 year, 10 months ago

Selected Answer: A

A

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward-proxy>

upvoted 3 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward-proxy>

upvoted 4 times

  **UFanat** 2 years, 2 months ago

Selected Answer: A

A. It's better to use Enterprise CA-signed cert

upvoted 3 times

  **alanouaro** 2 years, 8 months ago

Option A

(Best Practice) Enterprise CA-signed Certificates—An enterprise CA can issue a signing certificate that the firewall can use to sign the certificates for sites which require SSL decryption. When the firewall trusts the CA that signed the certificate of the destination server, the firewall can send a copy of the destination server certificate to the client, signed by the enterprise CA. This is a best practice because usually all network devices already trust the Enterprise CA (it is usually already installed in the devices' CA Trust storage), so you don't need to deploy the certificate on the endpoints, so the rollout process is smoother.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/configure-ssl-forward-proxy.html>

upvoted 4 times

  **Plato22** 2 years, 8 months ago

A is correct. Just tried on my lab Palo Alto.
upvoted 1 times

  **homersimpson** 2 years, 8 months ago

Yes it's A. cert needs to be a CA so it can create certs for each website visited, and cert needs to be enterprise-CA-signed so that windows clients will trust the certs created.
upvoted 1 times

Question #180

Topic 1

An administrator receives the following error message:

"IKE phase-2 negotiation failed when processing Proxy ID. Received local id 192. 168.33.33/24 type IPv4 address protocol 0 port 0, received remote id

172.16.33.33/24 type IPv4 address protocol 0 port 0."

How should the administrator identify the root cause of this error message?

- A. Verify that the IP addresses can be pinged and that routing issues are not causing the connection failure.
- B. Check whether the VPN peer on one end is set up correctly using policy-based VPN.
- C. In the IKE Gateway configuration, verify that the IP address for each VPN peer is accurate.
- D. In the IPsec Crypto profile configuration, verify that PFS is either enabled on both VPN peers or disabled on both VPN peers.

Correct Answer: B

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/vpns/set-up-site-to-site-vpn/interpret-vpn-error-messages.html>



  **Marshpillowz** 7 months, 1 week ago

Selected Answer: B

B is correct
upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

B. The VPN peer on one end is using policy-based VPN. You must configure a Proxy ID on the Palo Alto Networks firewall. See Create a Proxy ID to identify the VPN peers..
upvoted 1 times

  **lol12** 1 year, 10 months ago



Selected Answer: B

B
<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/vpns/set-up-site-to-site-vpn/interpret-vpn-error-messages>
upvoted 3 times


  **TAKUM1y** 1 year, 10 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/vpns/set-up-site-to-site-vpn/interpret-vpn-error-messages>
upvoted 3 times

  **Biz90** 2 years, 5 months ago

I know this too well from dealing with ASA to PAs! Answer is B.
upvoted 4 times

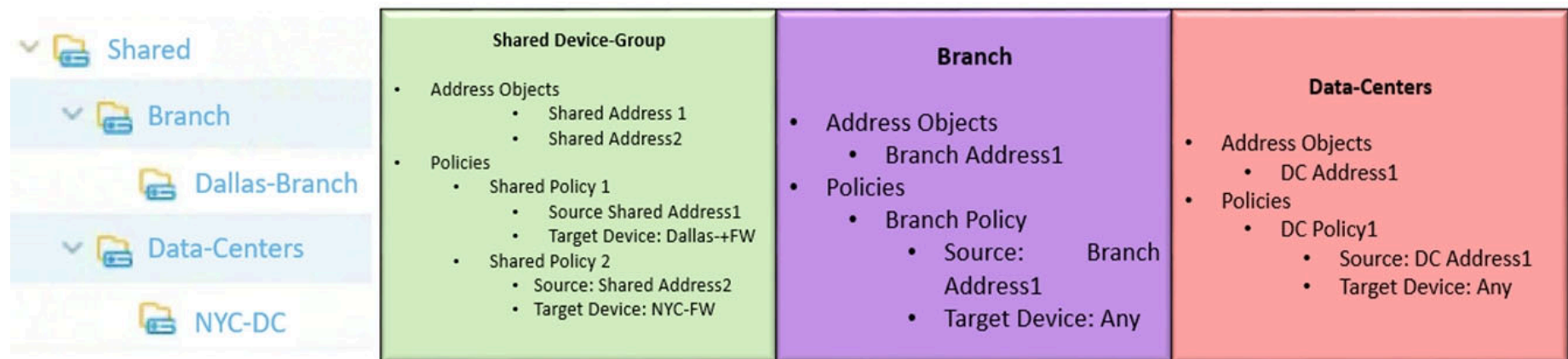
  **alanouaro** 2 years, 8 months ago

Option B
The VPN peer on one end is using policy-based VPN. You must configure a Proxy ID on the Palo Alto Networks firewall.
<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/vpns/set-up-site-to-site-vpn/interpret-vpn-error-messages.html>
upvoted 3 times

  **Plato22** 2 years, 8 months ago

B is correct. Cisco uses Policy based which is Proxy ID in Palo Alto
upvoted 2 times

The following objects and policies are defined in a device group hierarchy.



Dallas-Branch has Dallas-FW as a member of the Dallas-Branch device-group

NYC-DC has NYC-FW as a member of the NYC-DC device-group

What objects and policies will the Dallas-FW receive if "Share Unused Address and Service Objects" is enabled in Panorama?

- Address Objects -Shared Address1 -Branch Address1 Policies -Shared Policy1 -Branch Policy1
- Address Objects -Shared Address1 -Shared Address2 -Branch Address1 Policies -Shared Policy1 -Shared Policy2 -Branch Policy1
- Address Objects -Shared Address1 -Shared Address2 -Branch Address1 -DC Address1 Policies -Shared Policy1 -Shared Policy2 -Branch Policy1
- Address Objects -Shared Address1 -Shared Address2 -Branch Address1 Policies -Shared Policy1 -Branch Policy1

Correct Answer: D

homersimpson Highly Voted 2 years, 8 months ago

Selected Answer: D

Panorama will not push anything from Data-Centers group. That rules out C.

Panorama will push all objects from "Shared", which rules out A.

Note that the target of "Shared Policy 2" is NYC-FW, so this policy won't get pushed to Dallas-FW. This rules out B.

Thus, answer is D.

upvoted 11 times

Micutzu Highly Voted 2 years, 8 months ago

D is correct.

upvoted 5 times

Bighize 2 years, 8 months ago

I agree with Micutzu. I built this out in my lab. Dallas will not receive anything from the DataCenter Group. Only from the the shared and the Branch group. D is Correct.

upvoted 1 times

scanossa Most Recent 7 months ago

Selected Answer: D

Question asks about Dallas-FW, so every answer with "Shared Policy2" is discarded since it is related to NYC-FW

A is discarded because it does not have both address objects

D is the correct answer

upvoted 1 times

Marshpillowz 7 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times



ansibai 8 months, 2 weeks ago

Selected Answer: D

When you push configuration changes Device Groups, by default Panorama pushes all shared objects to firewalls whether or not any shared or device group policy rules reference the objects. However, you can configure Panorama to push only the shared objects that rules reference in the device groups. The Share Unused Address and Service Objects with Devices option enables you to limit the objects that Panorama pushes to the managed firewalls.

If "Share Unused Address and Service Objects with Device" is disabled/unchecked, Panorama evaluates unused objects while pushing configuration to the device. However this feature ignores the "target device" in security rules while evaluating unused objects.

upvoted 1 times

  **ansibai** 8 months, 2 weeks ago

Selected Answer: D

When you push configuration changes Device Groups, by default Panorama pushes all shared objects to firewalls whether or not any shared or device group policy rules reference the objects. However, you can configure Panorama to push only the shared objects that rules reference in the device groups. The Share Unused Address and Service Objects with Devices option enables you to limit the objects that Panorama pushes to the managed firewalls.

If "Share Unused Address and Service Objects with Device" is disabled/unchecked, Panorama evaluates unused objects while pushing configuration to the device. However this feature ignores the "target device" in security rules while evaluating unused objects.

upvoted 1 times



  **DatITGuyTho1337** 8 months, 2 weeks ago

Answer is "D" but I had to re-read the meaning of the "share unused address and service objects with devices" phrase because it is entirely COUNTER PRODUCTIVE to what it actually does. By default Panorama will share ALL objects whether or not they are used by members of the device group. Ticking the option above DISABLES that function forcing Panorama to only send objects that are used by the members of service groups. I swear a lot of PAN articles need proper grammar checks as they confuse learners. Even the aforementioned phrase should be changed to something like:

"DISABLE sharing unused address and service objects with devices"

See how much more clear that option now is? I think I will contact PAN customer support to factor this change. PAN tech is complicated enough, we don't need overly complicated grammar to make it even worse to understand!!!!

upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

Selected Answer: D

D. Because everything will be shared except for the shared policy 2, because it is targeting to share only with NYC-FW.

upvoted 1 times

  **Pretorian** 2 years ago

There's no "Branch Policy1" by the way...

upvoted 2 times

  **secdaddy** 2 years, 1 month ago

None of the above as the shared policy 1 has a typo in the target fw name (yes I know none of the above isn't an option)

upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: D

"Shared Policy 2" has set Target Device as NYC-FW, so Dallas-FW will never get it. (so B and C are not applicable)

Dallas-FW should also get both Shared Addresses 1 and 2 (So A is not applicable)

upvoted 1 times

  **AbuHussain** 2 years, 5 months ago

Selected Answer: D

D is correct.

upvoted 1 times

  **confusion** 2 years, 5 months ago

Selected Answer: D

Definitely D

upvoted 1 times

  **GivemeMoney** 2 years, 7 months ago

Selected Answer: D


Hard to freaking read, but yes answer is really D.

upvoted 2 times

  **anil4924** 2 years, 8 months ago



A is correct..

upvoted 1 times

  **Bighize** 2 years, 8 months ago

D is correct. I agree with Micutz. I built this out in my lab. Dallas will not receive anything from the DataCenter Group. Only from the the shared and the Branch group. D is Correct.

upvoted 1 times

  **Plato22** 2 years, 8 months ago

C is correct. It will receive everything under the Share.

upvoted 2 times

  **homersimpson** 2 years, 8 months ago

No, it will not receive Shared Policy 2 because that policy has a specific target of NYC.

upvoted 2 times

An administrator has purchased WildFire subscriptions for 90 firewalls globally.
What should the administrator consider with regards to the WildFire infrastructure?

- A. To comply with data privacy regulations, WildFire signatures and verdicts are not shared globally.
- B. Palo Alto Networks owns and maintains one global cloud and four WildFire regional clouds.
- C. Each WildFire cloud analyzes samples and generates malware signatures and verdicts independently of the other WildFire clouds.
- D. The WildFire Global Cloud only provides bare metal analysis.

Correct Answer: C

Reference:

<https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/wildfire-concepts/verdicts.html>

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: C

C is correct


upvoted 1 times

  **CertboxExam** 1 year, 8 months ago

Selected Answer: C

C is correct answer

upvoted 2 times

  **lol12** 1 year, 10 months ago

Selected Answer: C

C

<https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/wildfire-concepts/verdicts>

upvoted 4 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/wildfire-concepts/verdicts>

upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: C

C is correct

upvoted 2 times

  **alanouaro** 2 years, 8 months ago

Option C

Each WildFire cloud—global (U.S.), regional, and private—analyzes samples and generates WildFire verdicts independently of the other WildFire clouds. With the exception of WildFire private cloud verdicts, WildFire verdicts are shared globally, enabling WildFire users to access a worldwide database of threat data.

<https://docs.paloaltonetworks.com/wildfire/10-1/wildfire-admin/wildfire-overview/wildfire-concepts/verdicts.html>

upvoted 4 times

  **Plato22** 2 years, 8 months ago

C is correct.

upvoted 4 times

  **homersimpson** 2 years, 8 months ago

Agreed. B is wrong because there is no "global cloud". Just clouds for different regions, which don't share samples, but do share signatures and verdicts.

upvoted 3 times

A firewall is configured with SSL Forward Proxy decryption and has the following four enterprise certificate authorities (CAs): i. Enterprise-Trusted-CA, which is verified as Forward Trust Certificate (The CA is also installed in the trusted store of the end-user browser and system.) ii. Enterprise-Untrusted-CA, which is verified as Forward Untrust Certificate iii. Enterprise-Intermediate-CA iv. Enterprise-Root-CA, which is verified only as Trusted Root CA

An end-user visits <https://www.example-website.com/> with a server certificate Common Name (CN): www.example-website.com. The firewall does the SSL

Forward Proxy decryption for the website and the server certificate is not trusted by the firewall.

The end-user's browser will show that the certificate for www.example-website.com was issued by which of the following?

- A. Enterprise-Trusted-CA which is a self-signed CA
- B. Enterprise-Root-CA which is a self-signed CA
- C. Enterprise-Intermediate-CA which was, in turn, issued by Enterprise-Root-CA
- D. Enterprise-Untrusted-CA which is a self-signed CA

Correct Answer: D

  **Marcy** Highly Voted 2 years, 8 months ago

Should be D.
upvoted 5 times

  **homersimpson** Highly Voted 2 years, 8 months ago

Selected Answer: D

D is the answer.
upvoted 5 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: D

D is correct
upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward-proxy>
upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: D

Enterprise-Trusted-CA is installed in the trusted store of the end-user browser and system. So it should not lead to any certificate issue. The most possible that www.example-website.com is signed by not trusted certificate authority which leads to use Enterprise-Untrusted-CA, which is not trusted as well
upvoted 3 times

  **AbuHussain** 2 years, 5 months ago



Selected Answer: D

D is the answer
upvoted 1 times

  **GivemeMoney** 2 years, 7 months ago

Selected Answer: D

D. Enterprise-Untrusted-CA which is a self-signed CA
upvoted 3 times

  **Micutzu** 2 years, 8 months ago

D is correct
upvoted 4 times

What are three reasons for excluding a site from SSL decryption? (Choose three.)

- A. the website is not present in English
- B. unsupported ciphers
- C. certificate pinning
- D. unsupported browser version
- E. mutual authentication

Correct Answer: BCE

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/decryption-exclusions/exclude-a-server-from-decryption>



  **Marshpillowz** 7 months, 1 week ago

Selected Answer: BCE

B, C and E correct
upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

BCE. Reasons that sites break decryption technically include pinned certificates, client authentication, incomplete certificate chains, and unsupported ciphers. For HTTP public key pinning (HPKP), most browsers that use HPKP permit Forward Proxy decryption as long as you install the enterprise CA certificate (or the certificate chain) on the client.
upvoted 1 times

  **lol12** 1 year, 10 months ago

Selected Answer: BCE

BCE
<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-exclusions/exclude-a-server-from-decryption>
upvoted 3 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: BCE

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-exclusions/exclude-a-server-from-decryption>
upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: BCE

BCE are correct
upvoted 1 times

  **alanouaro** 2 years, 8 months ago

Options BCE
Reasons that sites break decryption technically include pinned certificates, client authentication, incomplete certificate chains, and unsupported ciphers.
<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/decryption-exclusions/exclude-a-server-from-decryption.html>
upvoted 4 times

DRAG DROP -

Match each SD-WAN configuration element to the description of that element.

Select and Place:

Answer Area

SD-WAN interface profile

Path Quality profile

Traffic Distribution profile

[Empty dashed box]

[Empty dashed box]

[Empty dashed box]

[Empty dashed box]

This profile or rule matches traffic to applications and services, sources, destinations, and users. The profile or rule indicates when and how the firewall performs application-based SD-WAN path selection

This profile or rule specifies how the firewall selects a new best path if the current preferred path exceeds a path quality threshold.

This profile or rule specifies the maximum latency, jitter, and packet loss thresholds.

This profile or rule specifies the tag that is applied to the physical interface. The profile or rule also specifies which type of Link that interface is.

Correct Answer:

Answer Area

SD-WAN interface profile

Path Quality profile

Traffic Distribution profile

SD-WAN interface profile

Traffic Distribution profile

Path Quality profile

SD-WAN interface profile

This profile or rule matches traffic to applications and services, sources, destinations, and users. The profile or rule indicates when and how the firewall performs application-based SD-WAN path selection

This profile or rule specifies how the firewall selects a new best path if the current preferred path exceeds a path quality threshold.

This profile or rule specifies the maximum latency, jitter, and packet loss thresholds.

This profile or rule specifies the tag that is applied to the physical interface. The profile or rule also specifies which type of Link that interface is.

axdrop Highly Voted 2 years, 8 months ago

Should be:

1. SD-WAN policy rule
2. Traffic Distribution profile
3. Path Quality profile
4. SD-WAN Interface profile

upvoted 21 times

Pretorian 2 years ago

"SD-WAN policy rule" is NOT an option

upvoted 1 times

  **Pretorian** 2 years ago

Nevertheless, axdrop's answers are correct. The question is messed up.



<https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/sd-wan-configuration-elements>

upvoted 2 times

  **Whizdhum** Most Recent 8 months, 3 weeks ago

All elements come together to create an SD-WAN Policy Rule ... this should be an option and matched to the first one. In either case, contributor axdrop is correct.

upvoted 1 times

  **sujss** 1 year, 4 months ago

If anyone is interested, found this short tutorial on Youtube.



<https://www.youtube.com/watch?v=ocRINJhsZ6M>

upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

<https://docs.paloaltonetworks.com/sd-wan/3-0/sd-wan-admin/sd-wan-overview/sd-wan-configuration-elements>

upvoted 2 times

  **NLT** 2 years, 6 months ago

Create a Path Quality profile for each set of business-critical and latency-sensitive applications, application filters, application groups, services, service objects and service group objects that has unique network quality (health) requirements based on latency, jitter, and packet loss percentage. Applications and services can share a Path Quality profile. Specify the maximum threshold for each parameter, above which the firewall considers the path deteriorated enough to select a better path.

upvoted 1 times

When overriding a template configuration locally on a firewall, what should you consider?

- A. Panorama will update the template with the overridden value.
- B. The firewall template will show that it is out of sync within Panorama.
- C. Only Panorama can revert the override.
- D. Panorama will lose visibility into the overridden configuration.

Correct Answer: D

scanossa 7 months ago

Selected Answer: D

Panorama still sees it as Sync but we still see the old setting
upvoted 1 times

Marshpillowz 7 months, 1 week ago

Selected Answer: D

D is correct
upvoted 1 times

DenskyDen 1 year, 7 months ago

D. Definitely. I already experience this.
upvoted 3 times

DenskyDen 1 year, 7 months ago

Selected Answer: D

D. Definitely. I already experience this.
upvoted 1 times

dogeatdog 1 year, 8 months ago

same as #421
upvoted 1 times

lol12 1 year, 10 months ago

Selected Answer: D

D for me unless revert is not the same as force template back to FW...
<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/templates-and-template-stacks>
upvoted 2 times

TAKUM1y 1 year, 10 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/templates-and-template-stacks>
upvoted 2 times

UFanat 2 years, 2 months ago

Selected Answer: D

Commit with force template values will override any setting made locally.
upvoted 1 times

Abu_Muhammad 2 years, 4 months ago

Selected Answer: B

I think it is B.
Losing visibility doesn't it mean that it will not be able to manage it any more?!
upvoted 1 times

lol12 1 year, 10 months ago

It's D.
From admin guide - Templates and Template Stacks.
When you override a setting on the firewall, the firewall saves that setting to its local configuration and Panorama no longer manages the setting.
upvoted 2 times

bartbernini 2 years, 7 months ago

Selected Answer: D



The correct answer is D.

"When you override a setting on the firewall, the firewall saves that setting to its local configuration and Panorama no longer manages the setting."
"If you push a configuration with Force Template Values enabled, all overridden values on the firewall are replaced with values from the template.
Before you use this option, check for overridden values on the firewalls to ensure your commit does not result in any unexpected network outages or issues caused by replacing those overridden values."

Although this doesn't explicitly indicate that you lose visibility, it definitely implies by advising you to check local firewall settings before forcing template values.

<https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/templates-and-template-stacks.html>

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/panorama-web-interface/panorama-commit-operations.html>
upvoted 4 times

  **rischa** 2 years, 7 months ago

Ans: B As per PCNSE study guide When you override the setting on the firewall, the firewall saves that setting to its local configuration and panorama no longer manages the setting.
upvoted 2 times

  **drrealest** 2 years, 8 months ago

it is A , Panorama allows you to override values a firewall received from a template and will let you know its a local value after youve changed it

<https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/override-a-template-setting/override-a-template-setting-on-the-firewall.html>
upvoted 2 times

  **drrealest** 2 years, 8 months ago

sorry B
upvoted 1 times

  **Mucho9999** 2 years, 8 months ago


Selected Answer: D

D is correct
upvoted 2 times

  **Micutzu** 2 years, 8 months ago

Based on my knowledge out-of-sync message appear on Panorama only was perform a commit to Panorama but not pushed to the NGFW.
<https://live.paloaltonetworks.com/t5/general-topics/reason-for-out-of-sync-message-in-panorama/td-p/328292>

The override setting are not visible (known) by Panorama. The config are pushed only from Panorama to NGFW.
I believe the correct answer is D.
upvoted 1 times

  **Plato22** 2 years, 8 months ago

Should be D.
upvoted 3 times


When setting up a security profile, which three items can you use? (Choose three.)

- A. Wildfire analysis
- B. anti-ransomware
- C. antivirus
- D. URL filtering
- E. decryption profile

Correct Answer: ACD

Reference:

<https://manualzz.com/doc/10741747/pan%E2%80%90administrator%E2%80%99s-guide-policy>

  **redgi0** 4 days, 7 hours ago

Antivirus
Anti-Spyware
Vulnerability Protection
URL Filtering
File Blocking
Wildfire Analysis
Data Filtering
DoS Protection
upvoted 1 times

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: ACD

A, C and D correct
upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: ACD

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/security-profiles>
upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: ACD

there is no antiransomware profile exists
decryption profile can be used in decryption policy
upvoted 1 times

  **fireb** 2 years, 3 months ago

Correct: A, C and D
upvoted 1 times

  **shinichi_88** 2 years, 7 months ago

should be - C
upvoted 1 times

  **alanouaro** 2 years, 8 months ago

Options ACD
<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/security-profiles.html>
upvoted 4 times

An administrator wants to upgrade a firewall HA pair to PAN-OS 10.1. The firewalls are currently running PAN-OS 8.1.17. Which upgrade path maintains synchronization of the HA session (and prevents network outage)?

- A. Upgrade directly to the target major version.
- B. Upgrade the HA pair to a base image.
- C. Upgrade one major version at a time.
- D. Upgrade two major versions at a time.

Correct Answer: C

Reference:


<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-upgrade/upgrade-pan-os/upgrade-the-firewall-pan-os/determine-the-upgrade-path.html>

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: C



C is correct

upvoted 1 times

  **DenskyDen** 1 year, 7 months ago



C. See TAKUM1y link.

upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

C. See TAKUM1y link.

upvoted 1 times

  **lol12** 1 year, 10 months ago

Selected Answer: C

Agree with C

upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/upgrade-pan-os/upgrade-the-firewall-pan-os/determine-the-upgrade-path>

upvoted 2 times

  **randomtotiti** 2 years, 3 months ago

In my opinion none of the answers are correct: when upgrading, the firewall will reboot and the cluster will run only on one member for a while, so no session synchronisation until it reboots.

upvoted 1 times

  **datz** 2 years, 3 months ago

Trust me, I did upgrade from 8.x to 10x and then when I did failover up upgrade secondary it went into suspended mode lol....so upgrade one major Version at a time :)

upvoted 1 times

  **alanouaro** 2 years, 8 months ago

Option C

When you upgrade from one PAN-OS feature release version to a later feature release, you cannot skip the installation of any feature release versions in the path to your target release. In addition, the recommended upgrade path includes installing the latest maintenance release in each release version before you install the base image for the next feature release version.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-upgrade/upgrade-pan-os/upgrade-the-firewall-pan-os/determine-the-upgrade-path.html>

upvoted 4 times

What are three types of Decryption Policy rules? (Choose three.)

- A. SSL Inbound Inspection
- B. SSH Proxy
- C. SSL Forward Proxy
- D. Decryption Broker
- E. Decryption Mirror

Correct Answer: ABC

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/decryption/decryption-overview.html#:~:text=The%20firewall%20provides%20three%20types,to%20control%20tunneled%20SSH%20traffic>

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: ABC

A, B and C correct
upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

ABC.

Create a Decryption policy rule to define traffic for the firewall to decrypt and the type of decryption you want the firewall to perform: SSL Forward Proxy, SSL Inbound Inspection, or SSH Proxy decryption. You can also use a Decryption policy rule to define Decryption Mirroring.



<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/define-traffic-to-decrypt/create-a-decryption-policy-rule>
upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

ABC.

Create a Decryption policy rule to define traffic for the firewall to decrypt and the type of decryption you want the firewall to perform: SSL Forward Proxy, SSL Inbound Inspection, or SSH Proxy decryption. You can also use a Decryption policy rule to define Decryption Mirroring.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/define-traffic-to-decrypt/create-a-decryption-policy-rule>
upvoted 1 times

  **lol12** 1 year, 10 months ago

Selected Answer: ABC


ABC as per admin guide

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-overview>
upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: ABC

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-overview>
upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: ABC

SSH Proxy, SSL Forward Proxy and SSL Inbound Inspection (if you posses a server certificate)
upvoted 1 times

  **Gilmarcio** 2 years, 7 months ago

A,B,C - <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/define-traffic-to-decrypt/create-a-decryption-policy-rule>
upvoted 3 times

During SSL decryption, which three factors affect resource consumption? (Choose three.)

- A. key exchange algorithm
- B. transaction size
- C. TLS protocol version
- D. applications ta non-standard ports
- E. certificate issuer

Correct Answer: ABC

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/prepare-to-deploy-decryption/size-the-decryption-firewall-deployment>

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: ABC

A, B and C correct
upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: ABC

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/prepare-to-deploy-decryption/size-the-decryption-firewall-deployment>
upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: ABC

Correct ABC
upvoted 2 times

  **shinichi_88** 2 years, 7 months ago

ABC are correct
upvoted 2 times

  **alanouaro** 2 years, 8 months ago

Options ABC
The encryption algorithm.
Average transaction sizes.
The TLS protocol version.
<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/prepare-to-deploy-decryption/size-the-decryption-firewall-deployment.html>
upvoted 2 times

An engineer must configure a new SSL decryption deployment.

Which profile or certificate is required before any traffic that matches an SSL decryption rule is decrypted?

- A. A Decryption profile must be attached to the Decryption policy that the traffic matches.
- B. There must be a certificate with both the Forward Trust option and Forward Untrust option selected.
- C. A Decryption profile must be attached to the Security policy that the traffic matches.
- D. There must be a certificate with only the Forward Trust option selected.

Correct Answer: D

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/configure-ssl-forward-proxy>

vansardo Highly Voted 2 years, 8 months ago

I think it is A. For example, in SSL Inbound Inspection you do SSL decryption and don't need Forward Trust or Untrust Certificate. You only need a decrypt policy with a decrypt profile.

upvoted 18 times

DavidBackham2020 2 years, 8 months ago

D is not false, but you still need a decryption profile for SSL Forward Proxy. A forward trust certificate alone is insufficient.

I agree with vansardo. The absolute minimum is the SSL Inbound Inspection profile (once the certificate and key are known to the firewall). Thus, A seems to be the most correct answer.

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/configure-ssl-inbound-inspection.html>

upvoted 3 times

Mp84047 2 years, 5 months ago

A is the correct answer

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/configure-ssl-inbound-inspection.html>

upvoted 3 times

secdaddy 2 years, 1 month ago

"(Optional) Select a Decryption Profile to perform additional checks on traffic that matches the policy rule."

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/define-traffic-to-decrypt/create-a-decryption-policy-rule>

upvoted 2 times

Micutzu Highly Voted 2 years, 8 months ago

I believe that in this case the correct answer is D.

I tested in my lab and isn't a must to have a Forward Untrust Certificate.

It's a must to have the Forward Trust Certificate defined.

Once you create a Decryption Policy Rule, you cannot commit without having a Forward Trust Certificate defined.

upvoted 8 times

BTSeeYa Most Recent 1 month, 2 weeks ago

Selected Answer: D

Yeah, this is just another terribly worded, "best answer" type question that makes people facepalm at cert tests.

If they just stated Forward Proxy in the question, then it would have to be D, but there is no Forward Trust cert used with inbound decryption.

Since decryption profiles are optional in either case, I'm going to have to assume they meant Forward Proxy and select D for my answer.

upvoted 1 times

Eluis007 4 months, 4 weeks ago

I believe Option A is the most suitable answer. Here's why: The question explicitly mentions "any traffic" to be decrypted, indicating both inbound and outbound scenarios. Therefore, it's crucial to have a solution capable of decrypting both inbound traffic and outbound traffic, whether it's directed towards trusted or untrusted destinations.

In this context, a decryption profile stands out as the most comprehensive solution. By attaching a decryption profile to the decryption policy rule, it ensures that all traffic matching the rule undergoes decryption, regardless of whether it's inbound or outbound, and regardless of the trust status of the destination server's certificate.

Hence, considering the broad scope of traffic mentioned in the question, Option A, which emphasizes the importance of a decryption profile, appears to be the most appropriate choice.

upvoted 1 times

cerifyme85 6 months, 1 week ago

Selected Answer: A

answer is A
upvoted 1 times

Marshpillowz 7 months, 1 week ago

Selected Answer: D

D appears to be correct
upvoted 1 times

Whizdhum 8 months, 3 weeks ago

Answer is D. At a minimum, you need a Forward Trust certificate to present to clients when a trusted CA has signed the server certificate. Although Decryption Policies are optional, it's a best practice to include them to prevent allowing questionable traffic on the network.
upvoted 1 times

Knowledge33 1 year, 2 months ago

Selected Answer: D

I just did it on my PAN. The decryption profile is not mandatory. It's optional, but the certificate with "forward trust" is mandatory.
upvoted 4 times

ConfuzedOne 1 year, 3 months ago

Selected Answer: D

I think this question / answer set must be entered incorrectly - the question/answer pairing itself is not complete - we need to know whether we're talking inbound SSL decryption or outbound SSL forward Proxy...

If it's inbound SSL decryption then then options B and D are completely bunk.

and as pointed out in some other comments, Palo's official documentation states decryption profiles are optional, but the question is about what is required. NO RIGHT ANSWER HERE

If this is for outbound SSL Forward Proxy, again, Palo's documentation says the profile is optional, so answers A and C are completely bunk.

Answer B completely defeats the purpose of the use of trusted and untrusted certificates - you need 2 certs, 1 trusted and 1 not trusted, so you would not have the same cert be both trusted and not trusted.

That leaves option D - There must be a certificate with only the Forward Trust option selected... so if there's anything close to right, it seems Option D is it.

upvoted 1 times

spitfire698 1 year, 4 months ago

D is correct.

you can create a decryption policy (ssl forward proxy) and leave the profile field in the policy on none. it will allow it, and traffic will still be decrypted.

(though I doubt it's a good idea to do it like that since at best in that case it will use the default profile which allows way too much, at worst is just doesn't apply any limitations at all)

upvoted 1 times

GohanF2 1 year, 6 months ago

A and D can be both true. However, I will go this time for D.

A is for additional granular control and it's not necessary for a regular SSL decryption rule . However, for deploying a regular SSL decryption rule, we need a trusted CA certificate to forward. <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-overview>

upvoted 1 times

John105 1 year, 7 months ago

I think A is correct, because D in the certificate option is not only 1 option possible to select as in point D. In addition to Forward Trust Certificate it possible options is Trusted Root CA. Therefore, A is correct Answer.

upvoted 1 times

mohr22 1 year, 7 months ago

A : After you create a decryption profile, attach it to a decryption policy rule; the firewall then enforces the decryption profile settings on traffic that matches the decryption policy rule.

upvoted 1 times

news088 1 year, 7 months ago

I think D is correct. The question come with must. To decrypt a decryption profile is not a requisite. But a certificate can only have one option trust or untrust not both. This is why D is the correct one.

upvoted 1 times

djedeen 1 year, 7 months ago

A:

Configuring SSL Inbound Inspection includes:

Installing the targeted server certificate on the firewall.

Creating an SSL Inbound Inspection Decryption policy rule.

Applying a Decryption profile to the policy rule.

upvoted 1 times

beikenes 1 year, 8 months ago

Selected Answer: A

A seems to be the most correct one

upvoted 3 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward-proxy>
upvoted 3 times

Question #192

Topic 1

Which two features require another license on the NGFW? (Choose two.)

- A. SSL Inbound Inspection
- B. SSL Forward Proxy
- C. Decryption Mirror
- D. Decryption Broker

Correct Answer: CD

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/configure-decryption-port-mirroring.html>

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-licenses.html>

  **GivemeMoney** **Highly Voted**  2 years, 7 months ago


Selected Answer: CD

C & D: However, you must activate a free license in order to enable Decryption Broker and Decryption Mirroring
upvoted 5 times

  **Marshpillowz** **Most Recent**  7 months, 1 week ago

Selected Answer: CD

C and D correct
upvoted 1 times

  **Whizdhum** 8 months, 3 weeks ago

Answers are C, D. Decryption Mirroring and Decryption Broker (Network Packet Broker) require a license. Both licenses are free and can be downloaded from the Customer Support Portal.

upvoted 1 times

  **PaloSteve** 1 year, 1 month ago

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-licenses>
In PAN-OS 10.1, the Decryption Broker feature and free license were replaced with Network Packet Broker.
This question has likely been removed from current tests.

upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: CD

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-licenses>
upvoted 4 times

  **RamanJoshi** 2 years, 7 months ago

C, D
<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/decryption-licenses.html>
upvoted 3 times

An administrator has a PA-820 firewall with an active Threat Prevention subscription. The administrator is considering adding a WildFire subscription.



How does adding the WildFire subscription improve the security posture of the organization?

- A. WildFire and Threat Prevention combine to minimize the attack surface.
- B. After 24 hours, WildFire signatures are included in the antivirus update.
- C. Protection against unknown malware can be provided in near real-time.
- D. WildFire and Threat Prevention combine to provide the utmost security posture for the firewall.

Correct Answer: C

  **Marcy** Highly Voted 2 years, 8 months ago

Should be C.
upvoted 10 times

  **Plato22** Highly Voted 2 years, 8 months ago

C is the correct answer. So many wrong answers on this site...
upvoted 8 times

  **Micutzu** 2 years, 8 months ago

It's not so bad to have also some bad answers because is forcing us to learn and not just memorize some answers :)
upvoted 12 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: C

C is correct
upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-overview/about-wildfire>
upvoted 2 times

  **AbuHussain** 2 years, 5 months ago

Selected Answer: C

Should be C.
upvoted 2 times

  **confusion** 2 years, 5 months ago

Selected Answer: C

Definitely C
upvoted 2 times

  **GivemeMoney** 2 years, 7 months ago

Selected Answer: C

Should be C HERE.
upvoted 4 times

What are two characteristic types that can be defined for a variable? (Choose two.)

- A. zone
- B. FQDN
- C. IP netmask
- D. path group

Correct Answer: BC

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/panorama-web-interface/panorama-templates/panorama-templates-template-variable.html>

  **alanouaro** Highly Voted 2 years, 8 months ago

Option BC
IP Netmask
FQDN

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/panorama-web-interface/panorama-templates/panorama-templates-template-variable.html>

upvoted 5 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: BC

B and C correct
upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: BC



<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-templates/panorama-templates-template-variable>

upvoted 3 times

  **UFanat** 2 years, 2 months ago

Selected Answer: BC

FQDN and IP Netmaks
upvoted 2 times

  **NLT** 2 years, 6 months ago

You can define variables (PanoramaTemplates) for templates and template stacks or you can edit existing variables for an individual device (PanoramaManaged DevicesSummary). Variables are configuration components defined on the template or template stack that provide flexibility and re-usability when you use Panorama to manage firewall configurations. You can use variables to replace:

An IP address (includes IP Netmask, IP Range, and FQDN) in all areas of the configuration.

Interfaces in an IKE Gateway configuration (Interface) and in an HA configuration (Group ID).

Configuration elements in your SD-WAN configuration (AS Number, QoS Profile, Egress Max, Link Tag).

upvoted 3 times


A remote administrator needs access to the firewall on an untrust interface. Which three options would you configure on an Interface Management profile to secure management access? (Choose three.)

- A. Permitted IP Addresses
- B. SSH
- C. https
- D. User-ID
- E. HTTP

Correct Answer: ABC

  **Marcy** Highly Voted 2 years, 8 months ago

It's ABC
upvoted 10 times



  **Plato22** Highly Voted 2 years, 8 months ago

ABC, how is enabling HTTP securing your access?
upvoted 7 times

  **Marshpillowz** Most Recent 7 months, 1 week ago

Selected Answer: ABC

A, B and C correct
upvoted 1 times

  **Sammy3637** 8 months, 4 weeks ago

Selected Answer: ABC

It's so obvious
upvoted 1 times

  **Aaronyukin** 1 year, 10 months ago

By obvious reasons it will be ABC. Others are insecure.
upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: ABC

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access>
upvoted 2 times

  **UFanat** 2 years, 2 months ago



Selected Answer: ABC

ABC
Do not use HTTP or Telnet for any management interface profile because those protocols transmit in cleartext.
<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access>
upvoted 1 times

  **AbuHussain** 2 years, 5 months ago

Selected Answer: ABC

It's ABC
upvoted 1 times

  **ev333** 2 years, 6 months ago

Selected Answer: ABC

Http is not secure
upvoted 1 times

  **Rloc20** 2 years, 7 months ago

BCD

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/configure-interfaces/use-interface-management-profiles-to-restrict-access.html>

upvoted 2 times

  **Mp84047** 2 years, 5 months ago

Its ABC, the doc you reference says that user-id is used to "Redistribute User Mappings and Authentication Timestamps"

upvoted 1 times

  **Elvenking** 2 years, 4 months ago

D can't be an answer because: "... and never enable HTTP or Telnet access because those protocols transmit in cleartext." as it is stated on the question that you should "secure" access, not just permit it.

Reference:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/networking/configure-interfaces/use-interface-management-profiles-to-restrict-access>

upvoted 1 times

  **RamanJoshi** 2 years, 7 months ago

A, B, C

upvoted 1 times

Question #196

Topic 1

An administrator needs to troubleshoot a User-ID deployment. The administrator believes that there is an issue related to LDAP authentication. The administrator wants to create a packet capture on the management plane.

Which CLI command should the administrator use to obtain the packet capture for validating the configuration?

- A. > scp export mgmt-pcap from mgmt.pcap to (username@host:path)
- B. > scp export poap-mgmt from poap.mgmt to (username@host:path)
- C. > ftp export mgmt-pcap from mgmt.pcap to <FTF host>
- D. > scp export pcap from pcap to (username@host:path)

Correct Answer: A

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleECAS>

  **K5000ism** Highly Voted  2 years, 7 months ago

Selected Answer: A

Additionally, you can manually export the PCAP via SCP or TFTP, i.e.:

```
> scp export mgmt-pcap from mgmt.pcap to  
<value> Destination (username@host:path)
```

Ref: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleECAS>


upvoted 6 times

  **Marshpillowz** Most Recent  7 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

Selected Answer: A

A. tested this.

upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: A

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleECAS>

upvoted 2 times

  **fireb** 2 years, 3 months ago

Correct

upvoted 2 times

When you configure an active/active high availability pair, which two links can you use? (Choose two.)

- A. 311
- B. Console Backup
- C. HSCI-C
- D. HA2 backup

Correct Answer: AD

Reference:


<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/set-up-activeactive-ha/configure-activeactive-ha.html>

  **Micutzu** Highly Voted 2 years, 8 months ago



HA3 and HA2 backup are correct choices.
upvoted 7 times

  **Micutzu** 2 years, 8 months ago

on PA-7000 has 2 HSCI ports (HSCI-A and HSCI-B), all the rest have only on HSCI port (if they have it). so HSCI-C it's not a valid answer. Also Console Port cannot be.
upvoted 5 times

  **techplus** 9 months, 2 weeks ago

Options are on test
HSCI-C
Console Port
HA3
HA2 backup
upvoted 3 times

  **Plato22** Highly Voted 2 years, 8 months ago

What is A supposed to be?
upvoted 6 times

  **Micutzu** 2 years, 8 months ago

on A it should be writtten HA3
upvoted 3 times

  **Marcy** 2 years, 8 months ago

I assume its HA3.
upvoted 1 times

  **FlamingPigeon** 2 years, 8 months ago

A is supposed to be HA3
upvoted 2 times

  **8f3e6ca** Most Recent 3 months ago

Poorly worded question. In essence they are asking any links that can be used, ar first glance it's easy to assume they are asking what links for just A/A. HA-3/HSCI is exclusive to A/A but A/A also requires HA-1 and HA-2 also so those are the links that can be used. Of those only HA-3 and HA-2 backup are present.
upvoted 1 times

  **cerifyme85** 6 months, 1 week ago

HA3

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/ha-links-and-backup-links#:~:text=HA1%20backup%20links-,Packet%2DForwarding%20Link,-In%20addition%20to>
upvoted 1 times

  **Marshpillowz** 7 months, 1 week ago

Selected Answer: AD



HA3 and HA2
upvoted 1 times

  **evilCorpBot7494** 7 months, 2 weeks ago

Selected Answer: AD


qwerqwer

upvoted 1 times

  **Whizdhum** 8 months, 3 weeks ago


Answers are A, D. Please correct choice A, as it should read HA3.

upvoted 1 times

  **Whizdhum** 8 months, 3 weeks ago



Also, the HSCI port can be used as an HA3 port on certain models, but there is no HSCI-C port. There are only HSCI-A and HSCI-B ports on the PA-7K specifically.

upvoted 1 times

  **lildevil** 1 year, 2 months ago

Odd question...i read it as physical links...no such thing as HA3 physical link...you either use the HSCI or a data plane port you have changed to type HA. I guess you could argue that HA2 backup is a valid option here...if it just means the names of the HA links then yes you obviously need HA2 (no backup needed) and HA3. Poor question.

upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: AD

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/set-up-activeactive-ha/prerequisites-for-activeactive-ha>

upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: AD

AD.

HA3 and HA2 backup are correct choices.

upvoted 2 times

What are two common reasons to use a "No Decrypt" action to exclude traffic from SSL decryption? (Choose two.)

- A. the web server requires mutual authentication
- B. the website matches a category that is not allowed for most users
- C. the website matches a high-risk category
- D. the website matches a sensitive category

Correct Answer: AD

Plato22 **Highly Voted** 2 years, 8 months ago

A and D:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/decryption/decryption-exclusions/create-a-policy-based-decryption-exclusion>

upvoted 11 times

Marcy **Highly Voted** 2 years, 8 months ago

Should be A and D

upvoted 8 times

samassier **Most Recent** 6 months, 2 weeks ago

D : Traffic that you should never decrypt because it contains personally identifiable information (PII) or other sensitive information, such as the URL Filtering categories financial-services, health-and-medicine, and government.

upvoted 1 times

Marshpillowz 7 months, 1 week ago

Selected Answer: AD

A and D correct

upvoted 1 times

evilCorpBot7494 7 months, 2 weeks ago

Selected Answer: AD

qwerqwer a d

upvoted 1 times

TAKUM1y 1 year, 10 months ago

Selected Answer: AD

A:<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-exclusions/exclude-a-server-from-decryption>

B:<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-exclusions/create-a-policy-based-decryption-exclusion>

upvoted 2 times

TAKUM1y 1 year, 10 months ago

Selected Answer: AD

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/decryption/decryption-exclusions/create-a-policy-based-decryption-exclusion>

upvoted 1 times

juan_L 2 years ago

A and D, no doubt.

A - Because decryption requires to proxy TLS and client certificate will not be used.

B- Compliance issues avoid to open tunnels to certain entities (...)

upvoted 2 times

UFanat 2 years, 2 months ago

Selected Answer: AD

Web server which requires mutual authentication does not support ssl decryption. And you should exclude sensitive sites from decryption.

upvoted 1 times

AbuHussain 2 years, 5 months ago

Selected Answer: AD

Should be A and D

upvoted 3 times

Micutzu 2 years, 8 months ago

For mutual authentication we must configure SSL Decryption Exclusion and once we include a destination into SSL Decryption Exclusion all the decryption policy rules are bypassed, therefor there is not action of "NO DECRYPT". "No decrypt" it's only inside decryption policy rule.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/decryption-exclusions/create-a-policy-based-decryption-exclusion.html>
"Traffic that originates or is destined for executives or other users whose traffic shouldn't be decrypted." = restricted/limited group of users

In my opinion the correct answers are B&D.

upvoted 5 times

  **Micutzu** 2 years, 8 months ago

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/decryption-exclusions/palo-alto-networks-predefined-decryption-exclusions.html>

The firewall provides a predefined SSL Decryption Exclusion list to exclude from decryption commonly used sites that break decryption because of technical reasons such as pinned certificates and mutual authentication.

upvoted 3 times

Question #199

Topic 1

PBF can address which two scenarios? (Choose two.)

- A. routing FTP to a backup ISP link to save bandwidth on the primary ISP link
- B. providing application connectivity the primary circuit fails
- C. enabling the firewall to bypass Layer 7 inspection
- D. forwarding all traffic by using source port 78249 to a specific egress interface

Correct Answer: AB

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/policy-based-forwarding/use-case-pbf-for-outbound-access-with-dual-isps>

  **prosto_marussia** Highly Voted  2 years, 7 months ago




Selected Answer: AB

D is wrong because PBF doesn't differentiate traffic by ports.

C doesn't make sense.

So A and B are correct.

upvoted 8 times

  **hpbdc** Highly Voted  1 year, 11 months ago

Selected Answer: AB

Port 78249... Really? lol :)

upvoted 5 times

  **Marshpillowz** Most Recent  7 months, 1 week ago

Selected Answer: AB

A and B correct

upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

Selected Answer: AB

This works like PBR in networking.

upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: AB

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/policy-based-forwarding/use-case-pbf-for-outbound-access-with-dual-isps>

upvoted 2 times

  **fireb** 2 years, 3 months ago

Correct options: A, B.

upvoted 1 times

A firewall should be advertising the static route 10.2.0.0/24 into OSPF. The configuration on the neighbour is correct, but the route is not in the neighbour's routing table.

Which two configurations should you check on the firewall? (Choose two.)

- A. Ensure that the OSPF neighbour state is "2-Way"
- B. In the OSPF configuration, ensure that the correct redistribution profile is selected in the OSPF Export Rules section.
- C. Within the redistribution profile ensure that Redist is selected.
- D. In the redistribution profile check that the source type is set to "ospf."

Correct Answer: B

Plato22 Highly Voted 2 years, 8 months ago

B and C. Question is asking to pick 2.
upvoted 7 times

Rtwf Highly Voted 2 years, 2 months ago

I took my exam today.
There was almost no question from here.
You need to have experience on PAN-OS 10.2
upvoted 6 times

Dilton 1 year, 6 months ago

Do you know where I could find a dump with question from exam? Thanks in advance
upvoted 4 times

327c7c8 Most Recent 5 months, 1 week ago

Selected Answer: B

B and C
upvoted 1 times

Marshpillowz 7 months, 1 week ago

B and C correct
upvoted 2 times

Whizdhum 8 months, 3 weeks ago

Answers are B, C. Please ensure that choice C shows as selected.
upvoted 2 times

DenskyDen 1 year, 7 months ago

BC. tested this.
upvoted 3 times

TAKUM1y 1 year, 10 months ago

Selected Answer: BC

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=KA10g000000CIGTCA0>
upvoted 3 times

datz 2 years, 3 months ago

B and C please :)
upvoted 2 times

fireb 2 years, 3 months ago

Correct options: B, C.
upvoted 2 times

IckoPCNSE 2 years, 3 months ago

Selected Answer: B

And C as well.
upvoted 1 times

AbuHussain 2 years, 5 months ago

B & C are correct.
upvoted 1 times


GivemeMoney 2 years, 7 months ago

B & C are correct.
upvoted 2 times

  **Mucho9999** 2 years, 8 months ago

B & C are correct.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIGTCA0>
upvoted 3 times

  **Marcy** 2 years, 8 months ago

B should be an answer I think.

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/network/network-virtual-routers/ospf/ospf-export-rules-tab>
upvoted 1 times

  **GivemeMoney** 2 years, 7 months ago

And C - two answers here.

upvoted 3 times

Question #201

Topic 1

Which value in the Application column indicates UDP traffic that did not match an App-ID signature?

- A. unknown-udp
- B. unknown-ip
- C. incomplete
- D. not-applicable

Correct Answer: A

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clc6CAC>

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/manage-custom-or-unknown-applications>

upvoted 1 times

  **Chandera** 2 years, 6 months ago

unknown-tcp or unknown-udp are connections where not enough data, or data that did not match any known applications's behavior for App-ID was unable to identify a known application... Correct Answer A

upvoted 3 times

What are three valid qualifiers for a Decryption Policy Rule match? (Choose three.)

- A. App-ID
- B. Custom URL Category
- C. User-ID
- D. Destination Zone
- E. Source Interface

Correct Answer: BCD

Reference:

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/define-traffic-to-decrypt/create-a-decryption-policy-rule>

  **TAKUM1y** Highly Voted  1 year, 10 months ago

Selected Answer: BCD



<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/define-traffic-to-decrypt/create-a-decryption-policy-rule>
upvoted 5 times

  **bouras** Most Recent  1 year ago

in version 11.0 i think there is also app-id
upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

BCD. See TAKUM1y link.
upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: BCD

BCD. There no App-ID or Source Interface options for decryption policy.
upvoted 4 times

  **GivemeMoney** 2 years, 7 months ago

BCD correct!
upvoted 3 times

  **Bryan1151** 2 years, 8 months ago

Selected Answer: BCD

Just check in lab
upvoted 4 times



An administrator needs to gather information about the CPU utilization on both the management plane and the data plane. Where does the administrator view the desired data?

- A. Resources Widget on the Dashboard
- B. Monitor > Utilization
- C. Support > Resources
- D. Application Command and Control Center

Correct Answer: A

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/dashboard/dashboard-widgets.html>

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/dashboard/dashboard-widgets>
upvoted 3 times

  **masa0102** 2 years, 1 month ago

A.easy

upvoted 2 times

Which CLI command displays the physical media that are connected to ethernet1/8?

- A. > show system state filter-pretty sys.s1.p8.stats
- B. > show system state filter-pretty sys.s1.p8.med
- C. > show interface ethernet1/8
- D. > show system state filter-pretty sys.s1.p8.phy

Correct Answer: D

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cld3CAC>

  **alanouaro** Highly Voted 2 years, 8 months ago

Option D

Example output:

```
> show system state filter-pretty sys.s1.p1.phy
```

```
sys.s1.p1.phy: {  
link-partner: {},  
media: CAT5,  
type: Ethernet,  
}
```

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cld3CAC>

upvoted 9 times

  **scanossa** Most Recent 8 months ago

I got this question on the exam

upvoted 4 times

  **brian7857ffs45** 9 months, 1 week ago

show system state filter-pretty sys.s1.

upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: D

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cld3CAC>

upvoted 3 times

  **UFanat** 2 years, 2 months ago

Selected Answer: D

D is a correct one

Checked in a lab

upvoted 3 times



A variable name must start with which symbol?

- A. \$
- B. !
- C. #
- D. &

Correct Answer: A

Reference:

<https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/configure-template-or-template-stack-variables.html>

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/configure-template-or-template-stack-variables>



upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: A

All variable definition names must start with the dollar sign (“\$”) character.

upvoted 1 times

  **fireb** 2 years, 3 months ago

Correct option: A.

upvoted 1 times


Given the following configuration, which route is used for destination 10.10.0.4? set network virtual-router 2 routing-table ip static-route "Route 1" nexthop ip-address 192.168.1.2 set network virtual-router 2 routing-table ip static-route "Route 1" metric 30 set network virtual-router 2 routing-table ip static-route "Route 1" destination 10.10.0.0/24 set network virtual-router 2 routing-table ip static-route "Route 1" re route-table unicast set network virtual-router 2 routing-table ip static-route "Route 2" nexthop ip-address 192.168.1.2 set network virtual-router 2 routing-table ip static-route "Route 2" metric 20 set network virtual-router 2 routing-table ip static-route "Route 2" destination 10.10.0.0/24 set network virtual-router 2 routing-table ip static-route "Route 2" route-table unicast set network virtual-router 2 routing-table ip static-route "Route 3" nexthop ip-address 10.10.20.1 set network virtual-router 2 routing-table ip static-route "Route 3" metric 5 set network virtual-router 2 routing-table ip static-route "Route 3" destination 0.0.0.0/0 set network virtual-router 2 routing-table ip static-route "Route 3" route-table unicast set network virtual-router 2 routing-table ip static-route "Route 4" nexthop ip-address 192.168.1.2 set network virtual-router 2 routing-table ip static-route "Route 4" metric 10 set network virtual-router 2 routing-table ip static-route "Route 4" destination 10.10.1.0/25 set network virtual-router 2 routing-table ip static-route "Route 4" route-table unicast

- A. Route 1
- B. Route 3
- C. Route 2
- D. Route 4

Correct Answer: C

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/network/network-virtual-routers/more-runtime-stats-for-a-virtual-router/routing-tab.html>

 **Whizdhum** 8 months, 3 weeks ago

Answer is C. It would be easier to format the configuration line-by-line, so that the four options are shown clearly. Nevertheless, I was able to sift through the jumbled configuration and find the answer.

upvoted 1 times

 **Knowledge33** 1 year, 3 months ago

Selected Answer: C

Longest mask first, then lowest metric is longest mask is concurrent.

upvoted 1 times

 **mbhuyan** 1 year, 6 months ago

Selected Answer: C

Opps my bed..the answer is C... longest has the different destination which is 10.10.1.0/25 I thought its 10.10.0.0/25.

upvoted 1 times

 **mbhuyan** 1 year, 6 months ago

Selected Answer: D

Longest match is 10.10.0.4 /25 which has the higher priority than /24. So the answer is D, not C

upvoted 1 times

 **hcir** 2 months, 1 week ago


mate, 10.10.1.0/25 matches 10.10.1.(0-127)

upvoted 2 times

 **djedeen** 1 year, 9 months ago

Route 3 has the lowest metric, but 1 & 2 are longer match than its 0.0.0.0/0 destination.

upvoted 1 times

 **Pakawat** 2 years, 2 months ago


Prefer route 2 with lowest metric

upvoted 2 times

 **secdaddy** 2 years, 1 month ago

longest match. lowest metric only comes into play if there is more than one route with the same length match.

upvoted 3 times

 **Jheax** 2 years, 4 months ago

Selected Answer: C

This is the line that you want to pay attention to answer this question:
set network virtual-router 2 routing-table ip static-route "Route 2" destination 10.10.0.0/24
upvoted 2 times

Question #207

Topic 1

In SSL Forward Proxy decryption, which two certificates can be used for certificate signing? (Choose two.)

- A. self-signed CA certificate
- B. server certificate
- C. wildcard server certificate
- D. client certificate
- E. enterprise CA certificate

Correct Answer: AE

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/configure-ssl-forward-proxy#:~:text=You%20can%20use%20an%20enterprise,as%20the%20forward%20trust%20certificate>

  **alanouaro** Highly Voted 2 years, 8 months ago

Options AE

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/configure-ssl-forward-proxy.html>



upvoted 6 times

  **TAKUM1y** Most Recent 1 year, 10 months ago

Selected Answer: AE

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward-proxy>

upvoted 3 times

  **UFanat** 2 years, 2 months ago

Selected Answer: AE

A and E are correct

upvoted 2 times

An administrator plans to deploy 15 firewalls to act as GlobalProtect gateways around the world. Panorama will manage the firewalls. The firewalls will provide access to mobile users and act as edge locations to on-premises infrastructure. The administrator wants to scale the configuration out quickly and wants all of the firewalls to use the same template configuration. Which two solutions can the administrator use to scale this configuration? (Choose two.)

- A. virtual systems
- B. template stacks
- C. variables
- D. collector groups

Correct Answer: AB

Reference:

<https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/templates-and-template-stacks>

  **Plato22**  2 years, 8 months ago

Another wrong answer. Should be B and C:

<https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/templates-and-template-stacks>

upvoted 15 times

  **Micutzu**  2 years, 8 months ago

B and C are correct!


upvoted 13 times

  **327c7c8**  5 months, 1 week ago

Selected Answer: BC

B and C

upvoted 1 times

  **Whizdhum** 8 months, 3 weeks ago

Answers are B, C. Clearly, this is a question about templates, template stacks and variables in Panorama. The key to answering this question is to understand template capabilities and exceptions. You cannot use templates or template stacks to set firewall modes, but as an exception, Panorama can push default vsys settings in a template to firewalls that don't support them or don't have any vsys configured. Since these PANs will be shipped world-wide, you will benefit from the use of variables to serve as placeholder objects based on configuration needs.

upvoted 2 times

  **Beluga123** 1 year, 4 months ago

Selected Answer: BC

Template Variables allow you to assign a dynamic value in a template configuration you can overwrite later in a template stack.

This can be particularly useful for IPv4 addresses you do not know value when configuring a template.

The IPv4 template variable can be referenced in different parts of the template configuration like in Global Protect configuration.

Procedure

When you are using IPv4 template variable for Gateway and/or Portal in Global Protect Configuration, you have to be sure this variable is also used to configure IP setting of the physical interface.

You have to verify this in Template configuration but also in Template stack configuration.

Template stack can contain more than one template, setting IPv4 configuration with conflicting values; the First template applied will prevail.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PO4UCAW>

upvoted 1 times

  **Rowdy_47** 1 year, 6 months ago

Selected Answer: BC

Cannot be A: Virtual systems are separate, logical firewall instances within a single physical Palo Alto Networks firewall. - FWs are being deployed around the world and acting as edge locations on premises



<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/virtual-systems/virtual-systems-overview>

Cannot be D: Panorama uses Log Collectors to aggregate logs from managed firewalls. When generating reports, Panorama queries the Log Collectors for log information, providing you visibility into all the network activity that your firewalls monitor.

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/centralized-logging-and-reporting/managed-collectors-and-collector-groups>

A Collector Group is 1 to 16 managed collectors that operate as a single logical log collection unit.

Therefore must be B and C which make the most sense
upvoted 1 times


  **drogce** 1 year, 10 months ago
B and C

You cannot use templates or template stacks to set firewall modes: multiple virtual systems (multi-vsys) mode
upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: AB

1 : <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/virtual-systems/virtual-systems-overview/benefits-of-virtual-systems>
//// 2 : <https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/templates-and-template-stacks>
upvoted 2 times

  **nolox** 3 months, 1 week ago

Yes, your 1st link speaks about scalability but it refers to general scalability. However for c2s vpn connections doesn't play a role, so I believe B & C are correct.
upvoted 1 times

  **GBD35055** 1 year, 10 months ago

I believe AB. Scalability is a benefit of Virtual Systems. Allows you to have multiple, separate firewalls in the same physical box.
<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/virtual-systems/virtual-systems-overview/benefits-of-virtual-systems#idcc37de80-c922-4762-97cf-66516a939cdf>
upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: BC

Template stacks and variables should be used. Collector Group is applicable only for panorama logging and make no sense for this question.
upvoted 1 times

  **Loloshikovichev** 2 years, 4 months ago

Selected Answer: BC

B and C are correct
upvoted 2 times

  **AbuHussain** 2 years, 5 months ago

Selected Answer: BC

Should be BC.
upvoted 2 times

  **GivemeMoney** 2 years, 7 months ago

Selected Answer: BD

Virtual systems and Variables don't make any sense with so many firewalls and sites and using panorama.
upvoted 3 times

  **GivemeMoney** 2 years, 7 months ago

Sorry i meant B and C!! ignore my first comment, i marked it as spam, hope it gets deleted.
upvoted 3 times

  **Marcy** 2 years, 8 months ago

Should be BC.
<https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/configure-template-or-template-stack-variables.html>
upvoted 6 times

Which three statements accurately describe Decryption Mirror? (Choose three.)

- A. Decryption, storage, inspection, and use of SSL traffic regulated in certain countries.
- B. You should consult with your corporate counsel before activating and using Decryption Mirror in a production environment.
- C. Decryption Mirror requires a tap interface on the firewall.
- D. Only management consent is required to use the Decryption Mirror feature.
- E. Use of Decryption Mirror might enable malicious users with administrative access to the firewall to harvest sensitive information that is submitted via an encrypted channel.

Correct Answer: ABE

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/decryption-concepts/decryption-mirroring>

  **UFanat** Highly Voted 2 years, 2 months ago

Selected Answer: ABE

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/decryption-concepts/decryption-mirroring>

Keep in mind that

- the decryption, storage, inspection, and/or use of SSL traffic is governed in certain countries and
- user consent might be required in order to use the decryption mirror feature.
- Additionally, use of this feature could enable malicious users with administrative access to the firewall to harvest usernames, passwords, social security numbers, credit card numbers, or other sensitive information submitted using an encrypted channel.
- Palo Alto Networks recommends that you consult with your corporate counsel before activating and using this feature in a production environment.

upvoted 6 times

  **betko** Most Recent 2 months, 2 weeks ago

This question was on exam in June 24.

upvoted 1 times

  **AbuHussain** 2 years, 5 months ago

Selected Answer: ABE

It;s ABE

upvoted 4 times

  **GivemeMoney** 2 years, 7 months ago

Selected Answer: ABE

B is right, which means D is wrong.
ABE is correct.



upvoted 4 times

  **blank_lv** 2 years, 8 months ago

Selected Answer: ABD

It;s ABD

upvoted 2 times

  **Mucho9999** 2 years, 8 months ago

Its definitely ABE.

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/decryption-concepts/decryption-mirroring.html>

upvoted 4 times

  **zicouille** 2 years, 8 months ago

It's ABE

upvoted 2 times

  **drrealst** 2 years, 8 months ago

"Keep in mind that the decryption, storage, inspection, and/or use of SSL traffic is governed in certain countries and user consent might be required in order to use the decryption mirror feature. Additionally, use of this feature could enable malicious users with administrative access to the firewall to harvest usernames, passwords, social security numbers, credit card numbers, or other sensitive information submitted using an encrypted channel. Palo Alto Networks recommends that you consult with your corporate counsel before activating and using this feature in a production environment."

upvoted 2 times

As a best practice, which URL category should you target first for SSL decryption?

- A. Health and Medicine
- B. High Risk
- C. Online Storage and Backup
- D. Financial Services

Correct Answer: B

Reference:

<https://docs.paloaltonetworks.com/best-practices/8-1/decryption-best-practices/decryption-best-practices/deploy-ssl-decryption-using-best-practices.html>

  **Davidpm** 1 year ago

Selected Answer: B



Plan to decrypt the riskiest traffic first (URL categories most likely to harbor malicious traffic, such as gaming or high-risk) and then decrypt more as you gain experience

<https://docs.paloaltonetworks.com/advanced-url-filtering/administration/configuring-url-filtering/url-filtering-best-practices>
upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/best-practices/10-2/decryption-best-practices/decryption-best-practices/plan-ssl-decryption-best-practice-deployment>
upvoted 3 times

  **datz** 2 years, 3 months ago

Interestingly Both seems to be BPA: This answer might have 2 answers in the exam.

Create policy to decrypt the rest of the traffic by configuring SSL Forward Proxy, SSL Inbound Inspection, and SSH Proxy rules. Always decrypt the online-storage-and-backup, web-based-email, web-hosting, personal-sites-and-blogs, content-delivery-networks, and high-risk URL categories.

<https://docs.paloaltonetworks.com/best-practices/10-1/decryption-best-practices/decryption-best-practices/deploy-ssl-decryption-using-best-practices>
upvoted 2 times



  **randomtotiti** 2 years, 3 months ago

Selected Answer: C

As a best practice the high-risk category should be blocked, leaving only C
upvoted 1 times


  **randomtotiti** 2 years, 3 months ago

Nevermind, it's B, my assumption that high-risk should be blocked as a BP was wrong
upvoted 1 times

  **Jheax** 2 years, 4 months ago

Selected Answer: B

Plan to decrypt the riskiest traffic first (URL Categories most likely to harbor malicious traffic, such as gaming or high-risk) and then decrypt more as you gain experience. Alternatively, decrypt the URL Categories that don't affect your business first (if something goes wrong, it won't affect business), for example, news feeds. - Taken from PANOS10 best practices found in <https://docs.paloaltonetworks.com/best-practices/10-0/decryption-best-practices/decryption-best-practices/plan-ssl-decryption-best-practice-deployment>
upvoted 2 times

  **Alen** 2 years, 4 months ago

Correct Answer is B. 'Online Storage and Backup is not a URL Category.
"Always decrypt the online-storage-and-backup, web-based-email, web-hosting, personal-sites-and-blogs, content-delivery-networks, and high-risk URL categories. Limit SSH Proxy to administrators who manage network devices, log all SSH traffic, and configure Multi-Factor Authentication to prevent unauthorized SSH access."
<https://docs.paloaltonetworks.com/best-practices/10-0/decryption-best-practices/decryption-best-practices/deploy-ssl-decryption-using-best-practices>
upvoted 1 times

  **Micutzu** 2 years, 8 months ago

The question is referring to URL categories used as best practice for SSL decryption, and not all URL categories.

Please read STEP 3 last bullet from here:

<https://docs.paloaltonetworks.com/best-practices/8-1/decryption-best-practices/decryption-best-practices/deploy-ssl-decryption-using-best-practices.html>

"If you can't decrypt everything, always decrypt the online-storage-and-backup, web-based-email, web-hosting, personal-sites-and-blogs, and content-delivery-networks URL categories."

upvoted 1 times

  **Micutzu** 2 years, 8 months ago

Starting with PAN-OS 9.0 the paragraph include also high-risk URL categories at the end of the list.

upvoted 2 times

  **Mucho9999** 2 years, 8 months ago

The test is based off of 10.0 High risk is the first to decrypt.

<https://docs.paloaltonetworks.com/best-practices/10-0/decryption-best-practices/decryption-best-practices/plan-ssl-decryption-best-practice-deployment.html>

upvoted 4 times

  **Hiwanku** 2 years, 8 months ago

Online Storage and Backup is not an URL category so option B

upvoted 2 times

  **Micutzu** 2 years, 8 months ago

please have a look here to see predefined URL categories:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm5hCAC>

Also, on URL filtering profile we can find Online-Storage-and-Back and High-Risk, at least in PAN-OS 10.x

upvoted 1 times


  **Micutzu** 2 years, 8 months ago

I suggest C as correct answer.

<https://docs.paloaltonetworks.com/best-practices/10-1/decryption-best-practices/decryption-best-practices/deploy-ssl-decryption-using-best-practices.html>

". Always decrypt the online-storage-and-backup, web-based-email, web-hosting, personal-sites-and-blogs, content-delivery-networks, and high-risk URL categories. ..."

upvoted 2 times

  **Mucho9999** 2 years, 8 months ago

Tricky question. Its B,

<https://docs.paloaltonetworks.com/best-practices/8-1/decryption-best-practices/decryption-best-practices/plan-ssl-decryption-best-practice-deployment.html>

Phase in decryption. Plan to decrypt the riskiest traffic first (URL Categories most likely to harbor malicious traffic, such as gaming or high-risk)

upvoted 2 times

Which User-ID mapping method should be used in a high-security environment where all IP address-to-user mappings should always be explicitly known?

- A. LDAP Server Profile configuration
- B. GlobalProtect
- C. Windows-based User-ID agent
- D. PAN-OS integrated User-ID agent

Correct Answer: D

  **Marcy** Highly Voted 2 years, 8 months ago

100% is B.

Because GlobalProtect users must authenticate to gain access to the network, the IP address-to-username mapping is explicitly known.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/user-id/user-id-concepts/user-mapping/globalprotect.html>


upvoted 22 times

  **GivemeMoney** 2 years, 7 months ago

B - This is the best solution in sensitive environments where you must be certain of who a user is in order to allow access to an application or service.

Thanks Marcy, you're awesome! So far you're right every time, i trust ya <3

upvoted 2 times

  **DatITGuyTho1337** 8 months, 1 week ago

yah but what does the GP infrastructure authenticate that information with? Surely not user and group information (nevermind user to IP address mappings) from AD, LDAP and the integrated PAN USER ID Agent!?!?!?



upvoted 2 times

  **327c7c8** Most Recent 5 months, 1 week ago

Selected Answer: B

GlobalProtect is the best method

upvoted 1 times

  **JRKhan** 7 months, 3 weeks ago

Selected Answer: B

B is correct. High sensitive environment, always on authentication, accurate/up to date user-to-ip mappings. And all the other options are not mapping methods.

upvoted 2 times

  **DatITGuyTho1337** 8 months, 1 week ago

Answer should be "C", because if AD which is extensively used in modern networks to administrate them does not know who users are then they either do not have access to network resources by default or they simply won't be able to login. The firewall groups info it authenticates to global protect users STILL MAKE USE OF AD. Never forget that!!!

upvoted 1 times

  **Waheeladawy** 1 year, 1 month ago

The answer is B. GlobalProtect.

GlobalProtect is a VPN solution that provides secure remote access to corporate networks. When a user connects to GlobalProtect, their identity is verified against an LDAP server. This ensures that all IP address-to-user mappings are explicitly known.

The other options are not as secure as GlobalProtect.

Option A, LDAP Server Profile configuration, allows for the configuration of multiple LDAP servers. This can make it difficult to track all IP address-to-user mappings.

Option C, Windows-based User-ID agent, relies on the Windows operating system to provide user identity. This can be less secure than using an LDAP server, as the Windows operating system is more susceptible to attack.

Option D, PAN-OS integrated User-ID agent, uses a local database to store user mappings. This database can be easily compromised, making it less secure than using an LDAP server.

upvoted 2 times

  **daytonadave2011** 1 year, 5 months ago

Selected Answer: B

B. GlobalProtect makes the most sense here because you're forcing the users to authenticate with GP before having access.

upvoted 3 times

  **Mauz88** 1 year, 6 months ago

B

Because GlobalProtect users must authenticate to gain access to the network, the IP address-to-username mapping is explicitly known. This is the best solution in sensitive environments where you must be certain of who a user is in order to allow access to an application or service.

upvoted 1 times

  **juan_L** 2 years ago

B,C and D are suitable for different reasons, let's see:

Global protect with always-on is the most secure option, all traffic will be encrypted to its gateway. Not everybody will have it installed so it's required to use in combination with other tool to force the installation, such as foscout... or a captive portal or what ever.


Windows based User-ID agent, The agent installation into an AD relay dedicated server is the most used, and allows to connect to multiple servers.

PAN-OS integrated is the last possible of this three, because it only permits to connect to a 1 server, if the environment has many AD or it have a connection problem, then you are in troubles, definitely this is not the preferable.

So finally the best choice is Global protect in combination of Win User-id app agent a good NAC if that security environment deserves.

... Ahora vas y lo cascás.

upvoted 3 times

  **UFanat** 2 years, 2 months ago

Selected Answer: B

key is "a high-security environment". In this case you should use zero trust approach with "authentication first", so you need to use GlobalProtect.

upvoted 4 times

  **AbuHussain** 2 years, 5 months ago

Selected Answer: B

It's B

upvoted 1 times

  **RamanJoshi** 2 years, 7 months ago

Guys, can anyone suggest where I can buy the best PCNSE dumps with correct answers

upvoted 3 times

  **alanouaro** 2 years, 8 months ago

Option B

Because GlobalProtect users must authenticate to gain access to the network, the IP address-to-username mapping is explicitly known. This is the best solution in sensitive environments where you must be certain of who a user is in order to allow access to an application or service.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/user-id/user-id-concepts/user-mapping/globalprotect.html>

upvoted 3 times

  **drrealest** 2 years, 8 months ago

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVPCA0>

"On sensitive and high security networks, WMI probing increases the overall attack surface, and administrators are recommended to disable WMI probing and instead rely upon User-ID mappings obtained from more isolated and trusted sources, such as domain controllers. If you are using the User-ID Agent to parse AD security event logs, syslog messages, or the XML API to obtain User-ID mappings, then WMI probing should be disabled. Captive portal can be used as a fallback mechanism to re-authenticate users where security event log data may be stale."

upvoted 1 times

  **Plato22** 2 years, 8 months ago

Wrong, there is no such thing as D.

Answer should be B or A

upvoted 1 times

  **RJ45TP** 2 years, 8 months ago

D does exist, though not saying it is correct

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-mapping-using-the-pan-os-integrated-user-id-agent>

upvoted 1 times

DRAG DROP -

Below are the steps in the workflow for creating a Best Practice Assessment in a firewall and Panorama configuration. Place the steps in order. Select and Place:

Answer Area

In either the NGFW or in Panorama, on the Operations/Support tab, download the technical support file.		Step 1
Log in to the Customer Support Portal (CSP) and navigate to Tools > Best Practice Assessment.		Step 2
Upload or drag and drop the technical support file.		Step 3
Map the zone type and area of the architecture to each zone.		Step 4
Follow the steps to download the BPA report bundle.		Step 5

Correct Answer:

Answer Area

	In either the NGFW or in Panorama, on the Operations/Support tab, download the technical support file.	Step 1
	Log in to the Customer Support Portal (CSP) and navigate to Tools > Best Practice Assessment.	Step 2
	Upload or drag and drop the technical support file.	Step 3
	Map the zone type and area of the architecture to each zone.	Step 4
	Follow the steps to download the BPA report bundle.	Step 5

Marcy Highly Voted 2 years, 8 months ago

Answer is all wrong.

Step 1. In either the NGFW or in Panorama, on the Operations/Support tab, download the technical support file.

Step 2. Log in to the Customer Support Portal (CSP) and navigate to Tools > Best Practice Assessment.

Step 3. Upload or drag and drop the technical support file.

Step 4. Map the zone type and area of the architecture to each zone.

Step 5. Follow the steps to download the BPA report bundle.

Reference:

<https://www.paloaltonetworks.com/resources/videos/how-to-run-a-bpa>

upvoted 23 times

  **GheeHong** 2 years, 1 month ago


ya, this is correct sequence.

upvoted 2 times

  **Sammy3637** Most Recent 8 months, 4 weeks ago

Looks like steps have been updated by the admin

upvoted 3 times

  **mercysayno765** 1 year, 2 months ago

Step 1. Log in to the Customer Support Portal (CSP) and navigate to Tools > Best Practice Assessment.

Step 2. In either the NGFW or in Panorama, on the Operations/Support tab, download the technical support file.

Step 3. Upload or drag and drop the technical support file.

Step 4. Map the zone type and area of the architecture to each zone.

Step 5. Follow the steps to download the BPA report bundle.

Reference:

<https://www.paloaltonetworks.com/resources/videos/how-to-run-a-bpa>

upvoted 2 times

  **TMoose** 2 years, 3 months ago

Q: How do I generate a BPA for NGFW/Panorama configurations?

A: Generate a BPA with the following steps:

Download the "tech support file" from the Operations/ Support tab of the NGFW and/or Panorama.

Login to Customer Support Portal(CSP) > Tools > Best Practice Assessment

Upload or drag and drop the Tech Support file.

Map the zone type and area of architecture to each zone.

Follow the steps to auto download the BPA report bundle.

upvoted 3 times

  **Alen** 2 years, 4 months ago



Dont see why step 1 and 2 cant be the other way round.

upvoted 4 times

  **network_geek_2020** 2 years, 7 months ago

Admin, Current answer is incorrect! please update with correct answers

upvoted 2 times

  **Plato22** 2 years, 8 months ago

Step 5 in the answer comes before Step 4.

upvoted 2 times

  **Marcy** 2 years, 8 months ago

<https://docs.paloaltonetworks.com/best-practices/9-0/best-practices-getting-started/get-started-with-best-practices/access-and-run-the-bpa.html>

upvoted 3 times

DRAG DROP -

Place the steps in the WildFire process workflow in their correct order.

Select and Place:

Answer Area

The firewall hashes the file and looks up a verdict in the WildFire database. However, the firewall does not find a match.		FIRST
WildFire uses static analysis based on machine learning to analyze the file, in order to classify malicious features.		SECOND
Regardless of the verdict, WildFire uses a heuristic engine to examine the file and determines that the file exhibits suspicious behavior.		THIRD
WildFire generates a new DNS, URL categorization, and antivirus signatures for the new threat.		FOURTH

Correct Answer:

Answer Area

		FIRST
	WildFire uses static analysis based on machine learning to analyze the file, in order to classify malicious features.	SECOND
	Regardless of the verdict, WildFire uses a heuristic engine to examine the file and determines that the file exhibits suspicious behavior.	THIRD
	WildFire generates a new DNS, URL categorization, and antivirus signatures for the new threat.	FOURTH

Reference:



<https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/about-wildfire.html>

Sammy3637 8 months, 4 weeks ago

left-->=Right
upvoted 1 times

Pretorian 2 years ago

Agreed, surprisingly, the provided answer is correct. Also the answers were given in the correct order in the first place.
upvoted 2 times

  **Jheax** 2 years, 4 months ago

The given answer is correct.

upvoted 3 times

In a Panorama template, which three types of objects are configurable? (Choose three.)

- A. certificate profiles
- B. HIP objects
- C. QoS profiles
- D. security profiles
- E. interface management profiles

Correct Answer: BDE

  **Marcy** Highly Voted 2 years, 8 months ago


It is ACE, anything under Network or device tabs is template.

- A. certificate profiles
- C. QoS profiles
- E. interface management profiles

B and D is under device-group.
upvoted 15 times

  **Plato22** Highly Voted 2 years, 8 months ago

Another wrong answer.
It's A, C and E.
upvoted 9 times

  **327c7c8** Most Recent 5 months, 1 week ago

Selected Answer: ABE

Under Panorama tab, the management profile, HIP and certificate are available, the other are available either under the template or device group which are not directly impact Panorama
upvoted 1 times

  **daytonadave2011** 1 year, 5 months ago

Selected Answer: ACE

ACE.
Template in Panorama is the Network and Device Tabs of your standalone firewall.
upvoted 2 times

  **duuduhast** 1 year, 7 months ago

Selected Answer: ACE

<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/use-case-configure-firewalls-using-panorama/set-up-your-centralized-configuration-and-policies/use-templates-to-administer-a-base-configuration>
upvoted 3 times

  **DenskyDen** 1 year, 7 months ago

Selected Answer: ACE

Tested it.
upvoted 1 times

  **bearfromdownunder** 1 year, 7 months ago

Selected Answer: ACE

<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/use-case-configure-firewalls-using-panorama/set-up-your-centralized-configuration-and-policies/use-templates-to-administer-a-base-configuration>
upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: ACE



HIP objects and Security Profiles - not in a template
upvoted 1 times

  **confusion** 2 years, 4 months ago

Selected Answer: ACE

100% ACE is correct.

upvoted 3 times

  **AbuHussain** 2 years, 5 months ago

Selected Answer: ACE

It is ACE

upvoted 4 times

  **prosto_marussia** 2 years, 7 months ago

Selected Answer: ACE

ACE indeed

upvoted 4 times

An internal system is not functioning. The firewall administrator has determined that the incorrect egress interface is being used. After looking at the configuration, the administrator believes that the firewall is not using a static route.

What are two reasons why the firewall might not use a static route? (Choose two.)

- A. duplicate static route
- B. no install on the route
- C. disabling of the static route
- D. path monitoring on the static route

Correct Answer: *BD*

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/static-routes/static-route-removal-based-on-path-monitoring.html>

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/static-routes/configure-a-static-route.html>

  **guy276465281819372** 3 months ago

Selected Answer: AD

A AND D. having duplicate routes is one of the most common mistakes.

upvoted 2 times

  **Chiquitabandita** 7 months, 1 week ago



I think A AND D since you can have a duplicate static route in the RIB but not in the FIB since the routes have different metrics/hops. I think this is a poorly written question and left out info related to the question. Or maybe it was transcribed incorrectly from the source, it just seem the question is incomplete and missing information

upvoted 3 times

  **DatITGuyTho1337** 8 months, 1 week ago

I chose "AD", because the "no install" option means that the admin never wanted to use that route. A duplicate static route can be configured with a different next hop and metric!

upvoted 3 times

  **Eluis007** 4 months, 4 weeks ago

If you configure another route with different next hop and metric, than you have two different routes, not duplicate routes!

upvoted 1 times

  **Marwansobhy** 11 months ago

you can no install in static routing by changing the unicast drop list to no install

upvoted 2 times



  **kalopilo** 1 year, 7 months ago

Ans: B & D.

When you Configure Path Monitoring for a Static Route, the firewall uses path monitoring to detect when the path to one or more monitored destination has gone down. The firewall can then reroute traffic using alternative routes. The firewall uses path monitoring for static routes much like path monitoring for HA or policy-based forwarding (PBF)



<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-networking-admin/static-routes/static-route-removal-based-on-path-monitoring>

upvoted 2 times

  **Sarbi** 1 year, 8 months ago

I am agreed there is no duplicate and disable routes

upvoted 1 times

  **Sarbi** 1 year, 8 months ago

How can path monitoring effects static routes?

upvoted 2 times

  **scanossa** 9 months, 2 weeks ago

Path monitoring could be detecting the next hop is down



upvoted 1 times

  **Lexus1323** 1 year, 8 months ago

Selected Answer: BD



you cant disabling a route and you can't create a duplicate static route

upvoted 2 times

  **mz101** 1 year, 9 months ago

If "duplicate static route" means same route with "different next hop", A could be the reason.



upvoted 3 times

  **UFanat** 2 years, 2 months ago

Selected Answer: BD

B and D

upvoted 2 times

  **NLT** 2 years, 6 months ago

When you Configure Path Monitoring for a Static Route, the firewall uses path monitoring to detect when the path to one or more monitored destination has gone down. The firewall can then reroute traffic using alternative routes.

upvoted 2 times



  **prosto_marussia** 2 years, 7 months ago

BD is correct

"No Install" is used if you do not want to install the route in the forwarding table.

And if path monitoring on the route fails it also won't be used

upvoted 2 times

  **DatITGuyTho1337** 8 months, 1 week ago

yes but why then be surprised that a second route doesn't work when it was not configured to be installed in the first place? I don't think the "no install" option is correct here.

upvoted 1 times

A customer is replacing its legacy remote-access VPN solution. Prisma Access has been selected as the replacement. During onboarding, the following options and licenses were selected and enabled:

- Prisma Access for Remote Networks: 300Mbps
- Prisma Access for Mobile Users: 1500 Users
- Cortex Data Lake: 2TB
- Trusted Zones: trust
- Untrusted Zones: untrust
- Parent Device Group: shared

The customer wants to forward to a Splunk SIEM the logs that are generated by users that are connected to Prisma Access for Mobile Users.

Which two settings must the customer configure? (Choose two.)

- A. Configure Panorama Collector group device log forwarding to send logs to the Splunk syslog server.
- B. Configure Cortex Data Lake log forwarding and add the Splunk syslog server.
- C. Configure a log forwarding profile and select the Panorama/Cortex Data Lake checkbox. Apply the Log Forwarding profile to all of the security policy rules in Mobile_User_Device_Group.
- D. Configure a Log Forwarding profile, select the syslog checkbox, and add the Splunk syslog server. Apply the Log Forwarding profile to all of the security policy rules in the Mobile_User_Device_Group.

Correct Answer: BC

Reference:

<https://docs.paloaltonetworks.com/cortex/cortex-data-lake/cortex-data-lake-getting-started/get-started-with-log-forwarding-app/forward-logs-from-logging-service-to-syslog-server.html>

  **DavidBackham2020** Highly Voted 2 years, 8 months ago

It's B&C. D would be correct for On-Prem firewalls, but you cannot directly forward Syslog from Prisma Access. You need to forward your logs to Cortex DL (C). From there, you can forward your logs to your SIEM (B)

<https://docs.paloaltonetworks.com/cortex/cortex-data-lake/cortex-data-lake-getting-started/get-started-with-log-forwarding-app/forward-logs-from-logging-service-to-syslog-server.html>

upvoted 8 times

  **p48m1** Highly Voted 1 year, 5 months ago

How is this related to the PCNSE? Isn't Cortex and Prisma part of the other dedicated certs?

upvoted 6 times

  **DatITGuyTho1337** Most Recent 8 months, 1 week ago

We learning for PCNSE or Prisma Access?!

upvoted 1 times

  **mopui5154** 2 years, 1 month ago

Hi, there is another version of This question :

What must be configured on Prisma Access to provide connectivity to the resources in the datacenter?



A-Configure a mobile user gateway in the region closest to the datacenter to enable connectivity to the datacenter

B-Configure a remote network to provide connectivity to the datacenter

C-Configure Dynamic Routing to provide connectivity to the datacenter

D-Configure a service connection to provide connectivity to the datacenter

upvoted 4 times

  **secdaddy** 1 year, 11 months ago

This has been added as question 296 in this dump

upvoted 1 times

  **secdaddy** 1 year, 11 months ago

Actually you're right - this question is still missing from examtopics (it is question 438 in the passleader dump)

upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: BC

Prisma Access can send logs only to Cortex Data Lake (CDL), so you need to select Panorama/CDL checkbox in log forwarding profile. Then you should configure CDL to forward logs to Splunk.

upvoted 2 times

  **AbuHussain** 2 years, 5 months ago

Selected Answer: BC

It's B&C

upvoted 2 times

  **Mp84047** 2 years, 5 months ago

It's definitely B & C. Its all from Prima so D makes no sense and David is right about not being able to forward directly


upvoted 1 times

  **Micutzu** 2 years, 8 months ago

I believe BD are correct.



Prisma Access forward all the logs to Cortex Data Lake by default.

upvoted 2 times

  **Marcy** 2 years, 8 months ago

Maybe its BC.. Not sure.

upvoted 1 times

  **Marcy** 2 years, 8 months ago

I think it's BD.

<https://docs.paloaltonetworks.com/cortex/cortex-data-lake/cortex-data-lake-getting-started/get-started-with-log-forwarding-app/forward-logs-from-logging-service-to-syslog-server.html#id186BM029099>

upvoted 2 times

  **Plato22** 2 years, 8 months ago

Agree, should be B and D. You have to pick your syslog server.

upvoted 2 times

  **confusion** 2 years, 1 month ago

Nope, the link you've provided is for forwarding logs from Cortex DL to Syslog server, the question is asking to forward logs from Prisma to SIEM syslog, so that shall not be applicable to the question. I think it's BC.

upvoted 1 times

A network administrator wants to use a certificate for the SSL/TLS Service Profile. Which type of certificate should the administrator use?

- A. machine certificate
- B. server certificate
- C. certificate authority (CA) certificate
- D. client certificate

Correct Answer: B

Marcy Highly Voted 2 years, 8 months ago

Should be
B. server certificate

Use only signed certificates, not CA certificates, in SSL/TLS service profiles.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/configure-an-ssl-tls-service-profile.html>
upvoted 12 times

Plato22 Highly Voted 2 years, 8 months ago

Another wrong answer. Should be B, common sense.
upvoted 6 times

DatITGuyTho1337 Most Recent 8 months, 1 week ago

I think the grammar is the confusing bit. I see server certificates as what external servers send to the firewall to establish a session. In fact in the below link someone else provided, the PAN team referred to it as a SIGNED CERTIFICATE. As such if one were to go with the options presented from face value, you are almost forced to select option C, whereas the PAN team really should use better grammar and just say signed certificates which is option B. Good lord!!

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/configure-an-ssl-tls-service-profile>
upvoted 1 times

Sammy3637 8 months, 4 weeks ago

Selected Answer: B

Server Certificate as it's a signed cert
upvoted 1 times

tomsui44 1 year, 3 months ago

Selected Answer: B

B - server cert. Ask your PKI admin to provide one in order to have a properly signed/valid cert. :)
upvoted 1 times

gugacalderaro 1 year, 6 months ago

Use only signed certificates, not CA certificates, in SSL/TLS service profiles.
upvoted 2 times

mohr22 1 year, 7 months ago

C In the client systems that request firewall services, the certificate trust list (CTL) must include the certificate authority (CA) certificate that issued the certificate specified in the SSL/TLS service profile. Otherwise, users will see a certificate error when requesting firewall services.
upvoted 1 times

mohr22 1 year, 7 months ago

C certificate authority (CA) certificate <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/configure-an-ssl-tls-service-profile>
upvoted 1 times

mohr22 1 year, 7 months ago

Sorry correct Ans is B server cert : <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/device/device-certificate-management-ssl-tls-service-profile>

in client it should be C Ca cert.

sorry for confusion
upvoted 1 times

djedeen 1 year, 7 months ago

Selected Answer: C

I think it is C, as you need a CA cert (enterprise PKI or external CA), else you are going to get cert warnings on the clients when connecting.
>>>

You must set up the certificate and SSL/TLS Service Profile on the PAN-OS system before you can connect using Privileged Access Service. Once the PAN-OS system is configured, the same certificate must also be trusted in all connector systems that are connected to the PAN-OS system. In most cases, PAN-OS systems should use a certificate obtained from an Enterprise Certificate Authority (CA), or a trusted external CA, like VeriSign. Since the certificate is trusted already, it simplifies the certificate setup on connector systems. You can also export the certificate from the PAN-OS system and import it into all systems running the connector. Self-signed certificates should not be used in production environments.
<<<

upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/configure-an-ssl-tls-service-profile>

upvoted 2 times

  **tenebrox** 2 years, 2 months ago

Selected Answer: B

It should be B

upvoted 3 times

  **UFanat** 2 years, 2 months ago

Selected Answer: B

It should be B as SSL/TLS Service Profile usually assigns to an IP which acts like a server, not client.
it should not be a CA from official docs:

Use only signed certificates, not CA certificates, in SSL/TLS service profiles.

upvoted 2 times

  **ManKing36** 2 years, 3 months ago

Selected Answer: B

answer is B

upvoted 3 times

  **AbuHussain** 2 years, 5 months ago

Selected Answer: B

Should be B

upvoted 2 times

  **shinichi_88** 2 years, 7 months ago

Selected Answer: B

fomr it is B

upvoted 1 times

In a security-first network, what is the recommended threshold value for content updates to be dynamically updated?

- A. 1 to 4 hours
- B. 6 to 12 hours
- C. 24 hours
- D. 36 hours

Correct Answer: B

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/threat-prevention/best-practices-for-content-and-threat-content-updates/best-practices-security-first.html#:~:text=In%20a%20security%2Dfirst%20network%2C%20schedule%20a,six%20to%20twelve%20hour%20threshold.&text=App%2DID%20Threshold-,,based%20on%20new%20App%2DIDs>

  **Marcy** Highly Voted 2 years, 8 months ago

B is correct.

Schedule content updates so that they download-and-install automatically. Then, set a Threshold that determines the amount of time the firewall waits before installing the latest content. In a security-first network, schedule a six to twelve hour threshold.

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/threat-prevention/best-practices-for-content-and-threat-content-updates/best-practices-security-first.html#id184AH00F06E>
upvoted 12 times

  **Bubu3k** Highly Voted 2 years, 4 months ago

Selected Answer: B

same for later versions of panos

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-upgrade/software-and-content-updates/best-practices-for-app-and-threat-content-updates/best-practices-security-first>
upvoted 6 times

  **Sammy3637** Most Recent 8 months, 4 weeks ago

Selected Answer: B



6-12 hours for Content updates

upvoted 1 times

  **brian7857ffs45** 9 months, 1 week ago

This question was on the exam.. Nov 2023

upvoted 2 times

  **news088** 1 year ago

Question was on my last exam

upvoted 3 times

  **tomsui44** 1 year, 3 months ago

That term "security-first network" is new to me. Thanks for the links! :)

upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-upgrade/software-and-content-updates/best-practices-for-app-and-threat-content-updates/best-practices-security-first>
upvoted 3 times

A network security engineer has applied a File Blocking profile to a rule with the action of Block. The user of a Linux CLI operating system has opened a ticket.

The ticket states that the user is being blocked by the firewall when trying to download a TAR file. The user is getting no error response on the system.



Where is the best place to validate if the firewall is blocking the user's TAR file?

- A. Threat log
- B. Data Filtering log
- C. WildFire Submissions log
- D. URL Filtering log

Correct Answer: B



Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIZ1CAK>

  **Sammy3637** 8 months, 4 weeks ago

Selected Answer: B

very obvious
it will be found in Data Filtering logs
upvoted 1 times

  **blahblah1234567890000** 1 year, 4 months ago

Selected Answer: B

View the file block logs in Data Filtering logs section. This is in the same Logs section as the Traffic and Threat logs under the Monitor tab. Navigate to Monitor > Logs > Data Filtering
upvoted 1 times

  **djedeen** 1 year, 7 months ago

Selected Answer: B

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIZ1CAK>

>>Resolution
View the file block logs in Data Filtering logs section. This is in the same Logs section as the Traffic and Threat logs under the Monitor tab.
upvoted 3 times

  **UFanat** 2 years, 2 months ago

Selected Answer: B

B. Data Filtering log
upvoted 2 times

  **K5000ism** 2 years, 7 months ago

Selected Answer: B

Navigate to Monitor > Logs > Data Filtering
upvoted 4 times

In a firewall, which three decryption methods are valid? (Choose three.)

- A. SSL Outbound Proxyless Inspection
- B. SSL Inbound Inspection
- C. SSH Proxy
- D. SSL Inbound Proxy
- E. Decryption Mirror

Correct Answer: BCE

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-overview.html>

  **Marcy** Highly Voted 2 years, 8 months ago


BCE is correct.
upvoted 7 times

  **123XYZT** Most Recent 3 months, 1 week ago

BCE
The firewall provides three types of Decryption policy rules: SSL Forward Proxy to control outbound SSL traffic, SSL Inbound Inspection to control inbound SSL traffic, and SSH Proxy to control tunneled SSH traffic. You can attach a Decryption profile to a policy rule to apply granular access settings to traffic, such as checks for server certificates, unsupported modes, and failures.
You can also use Decryption Mirroring to forward decrypted traffic as plaintext to a third party solution for additional analysis and archiving.
upvoted 1 times

  **Chiquitabandita** 7 months, 1 week ago

this answer conflicts with 189 on this list, decryption mirroring is counted as a rule profile or not? You can also use a Decryption policy rule to define Decryption Mirroring. On this question it is an answer and on 189 is not.
upvoted 1 times

  **Sammy3637** 8 months, 4 weeks ago

Selected Answer: BCE

Nothing exist as A&B , leaves us with options BCE
upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

BCE. The firewall provides three types of Decryption policy rules: SSL Forward Proxy to control outbound SSL traffic, SSL Inbound Inspection to control inbound SSL traffic, and SSH Proxy to control tunneled SSH traffic. You can attach a Decryption profile to a policy rule to apply granular access settings to traffic, such as checks for server certificates, unsupported modes, and failures. You can also use Decryption Mirroring to forward decrypted traffic as plaintext to a third party solution for additional analysis and archiving.
upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: BCE

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-overview>
upvoted 3 times

  **UFanat** 2 years, 2 months ago

Selected Answer: BCE

BCE correct
upvoted 2 times

  **K5000ism** 2 years, 7 months ago

Selected Answer: BCE

SSL Forward Proxy
SSL Inbound Inspection.
SSH Proxy

You can also use Decryption Mirroring to forward decrypted traffic as plaintext to a third party solution for additional analysis and archiving.

Ref: <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-overview.html#idd71f8b4d-cd40-4c6c-905f-2f8c7fca6537>

upvoted 4 times

DRAG DROP -

Match each type of DoS attack to an example of that type of attack.

Select and Place:

Answer Area

<div style="border: 1px solid black; padding: 5px; width: fit-content;">application-based attack</div>		<div style="border: 2px dashed blue; padding: 5px; width: fit-content;"></div>	Slowloris attack
<div style="border: 1px solid black; padding: 5px; width: fit-content;">protocol-based attack</div>		<div style="border: 2px dashed blue; padding: 5px; width: fit-content;"></div>	SYN flood attack
<div style="border: 1px solid black; padding: 5px; width: fit-content;">volumetric attack</div>		<div style="border: 2px dashed blue; padding: 5px; width: fit-content;"></div>	UDP flood attack

Correct Answer:

Answer Area

<div style="border: 1px solid black; padding: 5px; width: fit-content;"></div>		<div style="border: 2px dashed blue; padding: 5px; width: fit-content;">application-based attack</div>	Slowloris attack
<div style="border: 1px solid black; padding: 5px; width: fit-content;"></div>		<div style="border: 2px dashed blue; padding: 5px; width: fit-content;">protocol-based attack</div>	SYN flood attack
<div style="border: 1px solid black; padding: 5px; width: fit-content;"></div>		<div style="border: 2px dashed blue; padding: 5px; width: fit-content;">volumetric attack</div>	UDP flood attack

Reference:

<https://www.hackingarticles.in/dos-penetration-testing-part-1/#:~:text=Protocol%2DBased%20Attack%3A%20This%20kind,unresponsive%20to%20other%20legitimate%20requests>

- TAKUM1y Highly Voted 1 year, 10 months ago
<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense>
upvoted 6 times

- Cro13 Most Recent 2 months, 3 weeks ago
Answer is right

upvoted 1 times

  **BellaDrake** 2 years, 3 months ago

Correct... link to supporting documentation. <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense>

upvoted 4 times

Question #222

Topic 1

Using multiple templates in a stack to manage many firewalls provides which two advantages? (Choose two.)

- A. inherit address-objects from templates
- B. define a common standard template configuration for firewalls
- C. standardize server profiles and authentication configuration across all stacks
- D. standardize log-forwarding profiles for security polices across all stacks

Correct Answer: BC

  **Plato22** Highly Voted  2 years, 8 months ago

A and D are not part of the template.

Correct answer is B and C,

upvoted 7 times

  **Marcy** Highly Voted  2 years, 8 months ago

Should be BC.

upvoted 5 times

  **DenskyDen** Most Recent  1 year, 7 months ago

Selected Answer: BC

BC is the correct answer.

upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: BC

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/templates-and-template-stacks>

upvoted 4 times

  **UFanat** 2 years, 2 months ago

Selected Answer: BC

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/templates-and-template-stacks>

upvoted 2 times

  **AbuHussain** 2 years, 5 months ago

Should be BC.

upvoted 1 times

  **alanouaro** 2 years, 8 months ago

Selected Answer: BC

Template stacks simplify management because they allow you to define a common base configuration for all devices attached to the template stack and they give you the ability to layer templates to create a combined configuration.

upvoted 4 times





  **homersimpson** 2 years, 8 months ago

Selected Answer: BC

B+C because in D anything to do with log profiles are in the Objects tab, which is in Device Groups, not Templates.

upvoted 5 times

The SSL Forward Proxy decryption policy is configured. The following four certificate authority (CA) certificates are installed on the firewall.

<input type="checkbox"/>	NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGO...	USAGE
<input type="checkbox"/>	 Forward-Trust-Certificate	CN = Forward-Trust-Certificate	CN = Forward-Trust-Certificate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Feb 10 02:48:4...	valid	RSA	Forward Trust Certificate
<input type="checkbox"/>	 Forward-Untrust-Certificate	CN = Forward-Untrust-Certificate	CN = Forward-Untrust-Certificate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Feb 10 02:49:0...	valid	RSA	
<input type="checkbox"/>	 Firewall-CA	CN = Firewall-CA	CN = Firewall-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Feb 10 02:55:2...	valid	RSA	
<input type="checkbox"/>	 Firewall-Trusted-Root-CA	CN = Firewall-Trusted-Root-CA	CN = Firewall-Trusted-Root-CA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Feb 10 02:56:4...	valid	RSA	

An end-user visits the untrusted website <https://www.firewall-do-not-trust-website.com>.

Which certificate authority (CA) certificate will be used to sign the untrusted webserver certificate?

- A. Forward-Untrust-Certificate
- B. Forward-Trust-Certificate
- C. Firewall-CA
- D. Firewall-Trusted-Root-CA

Correct Answer: B

 **Abu_Muhammad** Highly Voted 2 years, 4 months ago

Selected Answer: B

B

Just simulated it:

(Operation

Validate

Status

Completed

Result

Successful

Warning: vsys1 decryption: forward decrypt untrust cert is not configured, forward decrypt trust cert will be used instead.)

upvoted 24 times

 **confusion** 2 years, 4 months ago

nice, thank you!

upvoted 1 times

 **Pretorian** 2 years ago

Wow, thank you!!

upvoted 1 times

 **Hiwanku** Highly Voted 2 years, 8 months ago


B, It is used by default when there is no untrusted in properties.

upvoted 11 times

 **drrealst** 2 years, 8 months ago

the usage column is blank for the untrusted one , so its not being used , so the trust one is used like you said

upvoted 1 times



 **Marcy** 2 years, 8 months ago

Can you provide a link to this please? I am having trouble finding it.

upvoted 2 times


 **weze1336** Most Recent 3 months ago

I don't get it. You are all saying that there is no "Forward-Untrust-Certificate",
But in the picture there is clearly a "Forward-Untrust-Certificate" So we know it's configured, So shouldn't the answer be A??
upvoted 1 times

  **Sammy3637** 8 months, 4 weeks ago

Selected Answer: B

keyword - 'user to sign'
upvoted 1 times

  **Sammy3637** 8 months, 2 weeks ago

type - 'used to sign'
upvoted 1 times

  **Lexus1323** 1 year, 8 months ago

Selected Answer: A



Additionally, set up a Forward Untrust certificate for the firewall to present to clients when the server certificate is signed by a CA that the firewall does not trust. This ensures that clients are prompted with a certificate warning when attempting to access sites with untrusted certificates.
upvoted 4 times

  **gc999** 10 months, 1 week ago

Yes, I see this from the link below, so why most of them people chose "B?"

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward-proxy>

upvoted 1 times

  **DatITGuyTho1337** 8 months, 1 week ago

Found this article that proves that if there is no forward untrust cert designated, the firewall is forced to use the designated forward trust certificate.

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000004NGkCAM&lang=en_US

upvoted 4 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/configure-ssl-forward-proxy>

upvoted 3 times

  **AbuHussain** 2 years, 5 months ago

Selected Answer: B

It's B

upvoted 3 times

  **Jared28** 2 years, 5 months ago

Selected Answer: B

It's B, I lab tested it. See the below reference, for those of you confused like I was, it says the untrust is required but apparently it's not (the comments here made me test it): <https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/configure-ssl-forward-proxy.html>
"After setting up the Forward Trust and Forward Untrust certificates required for SSL Forward Proxy decryption..."

upvoted 3 times

  **GivemeMoney** 2 years, 7 months ago

Selected Answer: B

B, Usage has forward trust certificate.

upvoted 3 times

  **zicouille** 2 years, 8 months ago

It's B, as there is no untrust set on properties

upvoted 2 times

  **alanouaro** 2 years, 8 months ago

Option A

Additionally, set up a Forward Untrust certificate for the firewall to present to clients when the server certificate is signed by a CA that the firewall does not trust. This ensures that clients are prompted with a certificate warning when attempting to access sites with untrusted certificates.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/configure-ssl-forward-proxy.html>

upvoted 2 times

  **Micutzu** 2 years, 8 months ago

Since Forward Trust Certificate isn't configured, then the Forward Trust Certificate will be used also for untrusted webserver.

Answer should be B. Forward-Trust-Certificate

upvoted 3 times

  **Marcy** 2 years, 8 months ago

This is not a good question. It isn't configured properly as there is no Untrusted Forward ticked. Does anyone know how to answer this?

upvoted 5 times

  **Breyarg** 2 years, 8 months ago

yes its B. and unfortunately seen this in production more than once.
upvoted 4 times

Question #224

Topic 1

A company needs to preconfigure firewalls to be sent to remote sites with the least amount of preconfiguration. Once deployed, each firewall must establish secure tunnels back to multiple regional data centers to include the future regional data centers.

Which VPN preconfigured configuration would adapt to changes when deployed to the future site?

- A. GlobalProtect client
- B. PPTP tunnels
- C. IPsec tunnels using IKEv2
- D. GlobalProtect satellite

Correct Answer: D

Reference:

<https://knowledgebase.paloaltonetworks.com/kCSArticleDetail?id=kA10g000000CIEQ>

  **alanouaro** Highly Voted  2 years, 8 months ago

Option D

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/globalprotect/network-globalprotect-portals/globalprotect-portals-satellite-configuration-tab.html>

upvoted 5 times

  **TAKUM1y** Most Recent  1 year, 10 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/globalprotect/network-globalprotect-portals/globalprotect-portals-satellite-configuration-tab>

upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: D

Option D




<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/globalprotect/network-globalprotect-portals/globalprotect-portals-satellite-configuration-tab.html>

upvoted 2 times

When an in-band data port is set up to provide access to required services, what is required for an interface that is assigned to service routes?

- A. You must set the interface to Layer 2, Layer 3, or virtual wire.
- B. The interface must be used for traffic to the required services.
- C. You must use a static IP address.
- D. You must enable DoS and zone protection.



Correct Answer: C

  **homersimpson** Highly Voted  2 years, 8 months ago

Selected Answer: C

ref: <https://live.paloaltonetworks.com/t5/general-topics/service-route-and-dhcp-interface/td-p/410874> "Only static ip addresses can be used for service routes." but B seems correct also since obviously the whole point of using that interface is that it has to be able to reach the service, do they mean traffic to the service and nothing else? I think the test writer needed another cup of coffee. I think C is the more clear-cut answer.

upvoted 14 times

  **sujs** 1 year, 4 months ago

B is a correct statement but not a valid answer for this question as it asks about the requirement specifically.

upvoted 1 times

  **Mucho9999** 2 years, 8 months ago

C is the most correct. <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clp3CAC>

upvoted 4 times

  **fzl96** 6 months, 2 weeks ago

yea the writer definitely needs a cup of coffee

upvoted 2 times

  **Jared28** Highly Voted  2 years, 5 months ago

Selected Answer: C

Definitely C. Service Route won't even list an interface not statically assigned as an option (verified in a lab as DHCP, no option, added a static IP and the interface appeared)

upvoted 5 times

  **ccaiccie** Most Recent  8 months, 2 weeks ago

Answer is B

upvoted 1 times

  **Sammy3637** 8 months, 4 weeks ago

Selected Answer: C

Service route needs static IP

upvoted 1 times

  **gc999** 10 months, 1 week ago


C is correct. I tested when I configured a static IP on ethernet1/1, then go to service route and I can choose ethernet1/1. However, once I change ethernet1/1 to use DHCP, then go to service route again, and there is no option for me for ethernet1/1. So static IP must exist for service route.

upvoted 2 times

  **ronin999** 2 years, 8 months ago

B is correct the service must be accessible by that dataplane port.

upvoted 2 times

  **DatITGuyTho1337** 8 months, 1 week ago

But it still needs a static route. I think answer B is superfluous.

upvoted 1 times

  **zicouille** 2 years, 8 months ago

Why not C ?

Decide which port you want to use for access to external services and connect it to your switch or router port.

The interface you use must have a static IP address. <=====

upvoted 1 times

  **drrealst** 2 years, 8 months ago



B cant be the right answer.. you can use the interface for data and mgmt. i'd say C

upvoted 1 times

  **drrealest** 2 years, 8 months ago

actually B is Correct. service routes are pointers so the interface Must be used for such use and other things

upvoted 1 times

  **DatITGuyTho1337** 8 months, 1 week ago

B is superfluous because the data plane is already used for traffic, using service routes just adds an additional traffic job for it. Answer C however is a requirement. The port will not function as a service route if its IP is via DHCP.

upvoted 1 times

Question #226

Topic 1




What does SSL decryption require to establish a firewall as a trusted third party and to establish trust between a client and server to secure SSL/TLS connection?

- A. link state
- B. profiles
- C. stateful firewall connection
- D. certificates

Correct Answer: D

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/decryption-overview.html>

  **TAKUM1y** Highly Voted  1 year, 10 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-overview>

"SSL decryption (both forward proxy and inbound inspection) requires certificates to establish the firewall as a trusted third party, and to establish trust between a client and a server to secure an SSL/TLS connection. You can also use certificates when excluding servers from SSL decryption for technical reasons (the site breaks decryption for reasons such as certificate pinning, unsupported ciphers, or mutual authentication). SSH decryption does not require certificates."

upvoted 5 times

  **DenskyDen** Most Recent  1 year, 7 months ago

Selected Answer: D

D.100%

upvoted 1 times

When you configure a Layer 3 interface, what is one mandatory step?

- A. Configure virtual routers to route the traffic for each Layer 3 interface.
- B. Configure Interface Management profiles, which need to be attached to each Layer 3 interface.
- C. Configure Security profiles, which need to be attached to each Layer 3 interface.
- D. Configure service routes to route the traffic for each Layer 3 interface.

Correct Answer: A

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/configure-interfaces/layer-3-interfaces.html>

  **TAKUM1y** Highly Voted  1 year, 10 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/configure-interfaces/layer-3-interfaces>

"In a Layer 3 deployment, the firewall routes traffic between multiple ports. Before you can Configure Layer 3 Interfaces, you must configure the virtual router that you want the firewall to use to route the traffic for each Layer 3 interface."

upvoted 5 times

  **Sammy3637** Most Recent  8 months, 4 weeks ago

Selected Answer: A

Virtual router is required 100%



upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: A

Zone and Virtual Router should be assigned to each L3 interface

upvoted 3 times

  **Roebi** 2 years, 5 months ago

A - Virtual Routers, without it you can't even close the configuration window

upvoted 3 times

  **K5000ism** 2 years, 7 months ago

Selected Answer: A

In a Layer 3 deployment, the firewall routes traffic between multiple ports. Before you can Configure Layer 3 Interfaces, you must configure the Virtual Routers that you want the firewall to use to route the traffic for each Layer 3 interface.

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/configure-interfaces/layer-3-interfaces.html>

upvoted 4 times

Which statement accurately describes service routes and virtual systems?

- A. Virtual systems can only use one interface for all global service and service routes of the firewall.
- B. Virtual systems that do not have specific service routes configured inherit the global service and service route settings for the firewall.
- C. Virtual systems cannot have dedicated service routes configured; and virtual systems always use the global service and service route settings for the firewall.
- D. The interface must be used for traffic to the required external services.

Correct Answer: B

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/virtual-systems/customize-service-routes-for-a-virtual-system>

  **homersimpson** Highly Voted 2 years, 8 months ago

Yes it's B: "When a firewall is enabled for multiple virtual systems, the virtual systems inherit the global service and service route settings." So you can define specific service routes if you want, but they start out as inherited from the global settings.

upvoted 8 times

  **TAKUM1y** Highly Voted 1 year, 10 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/virtual-systems/customize-service-routes-for-a-virtual-system>

"When a firewall is enabled for multiple virtual systems, the virtual systems inherit the global service and service route settings. For example, the firewall can use a shared email server to originate email alerts to all virtual systems. In some scenarios, you'd want to create different service routes for each virtual system."

upvoted 8 times

  **DenskyDen** Most Recent 1 year, 7 months ago

B. I concur.



upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: B

B is a correct answer

upvoted 2 times

  **NLT** 2 years, 6 months ago

When a firewall is enabled for multiple virtual systems, the virtual systems inherit the global service and service route settings. For example, the firewall can use a shared email server to originate email alerts to all virtual systems. In some scenarios, you'd want to create different service routes for each virtual system.

upvoted 4 times



An administrator is considering upgrading the Palo Alto Networks NGFW and central management Panorama version. What is considered best practice for this scenario?

- A. Perform the Panorama and firewall upgrades simultaneously.
- B. Upgrade the firewall first, wait at least 24 hours, and then upgrade the Panorama version.
- C. Upgrade Panorama to a version at or above the target firewall version.
- D. Export the device state, perform the update, and then import the device state.

Correct Answer: C

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRrCAK>

  **Marcy** Highly Voted 2 years, 8 months ago

C is correct.

Panorama should be running the same or a later version of a feature release than the firewall (more than two feature versions is supported but not recommended).

upvoted 8 times

  **GivemeMoney** 2 years, 7 months ago

C - Panorama should be upgraded first and same or newer version then the firewalls.

upvoted 2 times

  **Sammy3637** Most Recent 8 months, 4 weeks ago

Selected Answer: C

important step
always upgrade panorama first

upvoted 1 times


  **TAKUM1y** 1 year, 10 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/upgrade-pan-os/upgrade-the-firewall-pan-os/upgrade-firewalls-using-panorama>

"Make sure Panorama is running the same or a later PAN-OS version than you are upgrading to."

upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: C

C is correct. Panorama should be the same or higher version then firewalls

upvoted 2 times

An administrator has 750 firewalls. The administrator's central-management Panorama instance deploys dynamic updates to the firewalls. The administrator notices that the dynamic updates from Panorama do not appear on some of the firewalls. If Panorama pushes the configuration of a dynamic update schedule to managed firewalls, but the configuration does not appear, what is the root cause?

- A. Panorama does not have valid licenses to push the dynamic updates.
- B. Panorama has no connection to Palo Alto Networks update servers.
- C. Locally-defined dynamic update settings take precedence over the settings that Panorama pushed.
- D. No service route is configured on the firewalls to Palo Alto Networks update servers.

Correct Answer: C

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIKQCA0>

 **Marcy** Highly Voted 2 years, 8 months ago

C is correct.

C

C

C

C is correct.

Locally defined dynamic updates setting on a managed Palo Alto Networks firewall take preference over the Panorama pushed setting.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIKQCA0>

upvoted 6 times

 **TAKUM1y** Most Recent 1 year, 10 months ago

Selected Answer: C

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIKQCA0>

"Locally defined dynamic updates setting on a managed Palo Alto Networks firewall take preference over the Panorama pushed setting."

upvoted 4 times

An enterprise Information Security team has deployed policies based on AD groups to restrict user access to critical infrastructure systems. However, a recent phishing campaign against the organization has prompted information Security to look for more controls that can secure access to critical assets. For users that need to access these systems, Information Security wants to use PAN-OS multi-factor authentication (MFA) integration to enforce MFA.

What should the enterprise do to use PAN-OS MFA?

- A. Use a Credential Phishing agent to detect, prevent, and mitigate credential phishing campaigns.
- B. Create an authentication profile and assign another authentication factor to be used by a Captive Portal authentication policy.
- C. Configure a Captive Portal authentication policy that uses an authentication sequence.
- D. Configure a Captive Portal authentication policy that uses an authentication profile that references a RADIUS profile.

Correct Answer: D

  **homersimpson** Highly Voted 2 years, 8 months ago

FYI in 10.0 onward, "Captive Portal" is now called "Authentication Portal".
upvoted 9 times

  **JRKhan** Highly Voted 7 months, 3 weeks ago

Selected Answer: B


B is correct. Given the authentication using AD is already in place, we can safely assume that LDAP server profile is already in use. The MFA will be used as an additional/second authentication factor. Also, the question refers to PAN-OS MFA so it is again safe to assume it will use PAN-OS directly integrated vendors instead of using one through RADIUS.
upvoted 7 times

  **jeremykebir** 2 months, 1 week ago

Abolutely right!
upvoted 1 times

  **Nicoara** Most Recent 4 weeks ago

I believe is C. because the authentication sequence can include multiple authentication methods, which is essential for implementing MFA.
upvoted 1 times

  **Whizdhum** 8 months, 3 weeks ago

Answer is D. To use MFA for protecting sensitive information, you must configure an Authentication Portal (Captive Portal) to display a web form. To enable additional factors, you can integrate with MFA vendors through RADIUS or vendor APIs. In most cases, and external service is recommended for the first authentication factor.
upvoted 1 times



  **Eiffelsturm** 9 months ago

Selected Answer: D

B and C are the same except that B offers more options for the authentication factors in the authentication profile. "Add a RADIUS server profile. This is required if the firewall integrates with an MFA vendor through RADIUS" since D is more granular, I go for D
upvoted 1 times

  **Gabbranch** 9 months ago

I feel like RADIUS is the work-around for those MFA solutions that don't natively integrate with PAN-OS. And the question asks about PAN-OS MFA Integration. That's why I think C over B.
upvoted 2 times

  **gc999** 10 months, 1 week ago

Selected Answer: D

Would the keyword here is "PAN-OS MFA"? I see the word from the following UR

"For remote user authentication to GlobalProtect portals or gateways or for administrator authentication to the PAN-OS or Panorama web interface, you can only use MFA vendors supported through RADIUS or SAML"

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/authentication/configure-multi-factor-authentication#:~:text=you%20can%20only%20use%20MFA%20vendors%20supported%20through%20RADIUS%20or%20SAML>
upvoted 1 times

  **josephrahul** 1 year, 1 month ago

Option D

To use Multi-Factor Authentication (MFA) for protecting sensitive services and applications, you must configure Authentication Portal to display a web form for the first authentication factor and to record Authentication Timestamps. The firewall uses the timestamps to evaluate the timeouts for

Authentication Policy rules. To enable additional authentication factors, you can integrate the firewall with MFA vendors through RADIUS or vendor APIs.

upvoted 1 times

  **dgonz** 1 year, 1 month ago

Selected Answer: B

i think B is closer

upvoted 2 times

  **Techn** 1 year, 1 month ago

Selected Answer: D

For end-user authentication via the Authentication policy, the firewall directly integrates with several MFA platforms (such as Duo v2, Okta Adaptive, PingID, and RSA SecurID) and integrates through RADIUS with other MFA platforms.

upvoted 1 times

  **ericli87** 1 year, 5 months ago

did anyone see this in the exam?

upvoted 5 times

  **Pochex** 1 year, 5 months ago

Answer B

When we use PANOS MFA, the user will first authenticate with the authentication profile configured (Radius, SAML, Kerberos, TACACS+, LDAP), then an additional factor is configured in the same authentication profile, this factor is the MFA which is used by the Captive Portal.

upvoted 4 times

  **Frightened_Acrobat** 1 year, 5 months ago

Selected Answer: B

B and D are both wrong -Authentication policies reference Authentication Enforcement policies directly, not Authentication profiles. However, if one of them has to be right, it's B. D is less right since RADIUS isn't the only MFA option.

upvoted 5 times

  **magicbr3** 8 months ago

The Captive portal can reference the RADIUS profile and you configure MFA in the captive portal

upvoted 1 times

  **mohr22** 1 year, 7 months ago

D To use Multi-Factor Authentication (MFA) for protecting sensitive services and applications, you must configure Authentication Portal to display a web form for the first authentication factor and to record Authentication Timestamps. The firewall uses the timestamps to evaluate the timeouts for Authentication Policy rules. To enable additional authentication factors, you can integrate the firewall with MFA vendors through RADIUS or vendor APIs.



upvoted 1 times

  **TAKUM1y** 1 year, 9 months ago

Selected Answer: D



<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/authentication/configure-multi-factor-authentication>

upvoted 6 times

  **scally** 1 year, 11 months ago

To use Multi-Factor Authentication (MFA) for protecting sensitive services and applications, you must configure Captive Portal to display a web form for the first authentication factor and to record Authentication Timestamps. The firewall uses the timestamps to evaluate the timeouts for Authentication Policy rules. To enable additional authentication factors, you can integrate the firewall with MFA vendors through RADIUS or vendor APIs. After evaluating Authentication policy, the firewall evaluates Security policy, so you must configure rules for both policy types.

upvoted 3 times

  **UFanat** 2 years, 2 months ago

Selected Answer: B

You should create an auth profile and use it in captive portal auth policy.

upvoted 4 times

  **Marcy** 2 years, 8 months ago

D sounds the most correct from this line in the link.

To use Multi-Factor Authentication (MFA) for protecting sensitive services and applications, you must configure Captive Portal to display a web form for the first authentication factor and to record Authentication Timestamps. The firewall uses the timestamps to evaluate the timeouts for Authentication Policy rules. To enable additional authentication factors, you can integrate the firewall with MFA vendors through RADIUS or vendor APIs. After evaluating Authentication policy, the firewall evaluates Security policy, so you must configure rules for both policy types.

upvoted 3 times

  **homersimpson** 2 years, 8 months ago

I think it's B, because with D you are referencing Radius, which doesn't necessarily imply you're using another factor. With B, you might not have had an auth profile already (since you don't need one with user/pwd auth) so you would be creating one, and you would assign another factor in it. FWIW, this question is poorly worded.

upvoted 11 times

[-] 👤 **GivemeMoney** 2 years, 7 months ago
Radius is one option, not "Thee" option, It's B.
upvoted 3 times

[-] 👤 **Shenanigans123** 2 years, 5 months ago
I agree with this. Also, D says the Authentication Profile should reference a RADIUS server profile - this would make the primary auth method RADIUS, whereas the question states they want to use AD groups as the primary method, so the profile should use LDAP as the first factor, then add MFA as a second factor. D also does not mention any additional factor.

B covers all requirements.
upvoted 2 times

[-] 👤 **Gngogh** 1 year, 10 months ago
I just want to highlight that you don't have to use LDAP as first authentication method to be able to retrieve the user groups. In fact, in many deployments RADIUS server queries the AD server for user authentication. Then the firewall if properly configured will do the group mappings. Regardless I also believe the correct answer is B, because has already mentioned it covers all use cases.
upvoted 1 times

Question #232

Topic 1

An administrator wants to enable zone protection.
Before doing so, what must the administrator consider?

- A. Activate a zone protection subscription.
- B. Security policy rules do not prevent lateral movement of traffic between zones.
- C. The zone protection profile will apply to all interfaces within that zone.
- D. To increase bandwidth, no more than one firewall interface should be connected to a zone.

Correct Answer: C

Reference:

<https://live.paloaltonetworks.com/t5/general-topics/apply-zone-protection-to-which-zone/td-p/36113>

[-] 👤 **TAKUM1y** 1 year, 10 months ago
Selected Answer: C
<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/how-do-zones-protect-the-network>
upvoted 2 times

[-] 👤 **UFanat** 2 years, 2 months ago
Selected Answer: C
Zone protection profile applies to all zone interfaces
upvoted 2 times

[-] 👤 **mysteryzjoker** 2 years, 4 months ago
C is correct
upvoted 3 times

When you import the configuration of an HA pair into Panorama, how do you prevent the import from affecting ongoing traffic?

- A. Disable HA.
- B. Disable the HA2 link.
- C. Set the passive link state to "shutdown."
- D. Disable config sync.

Correct Answer: D

Reference:

<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/transition-a-firewall-to-panorama-management/migrate-a-firewall-ha-pair-to-panorama-management.html>

  **homersimpson** Highly Voted  2 years, 8 months ago

Updated reference: <https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/manage-firewalls/transition-a-firewall-to-panorama-management/migrate-a-firewall-ha-pair-to-panorama-management.html>. Step 2 is "Disable configuration synchronization between the HA peers."
upvoted 7 times

  **TAKUM1y** Most Recent  1 year, 10 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/transition-a-firewall-to-panorama-management/migrate-a-firewall-ha-pair-to-panorama-management>
upvoted 4 times

  **UFanat** 2 years, 2 months ago

Selected Answer: D

D. Disable config sync.
upvoted 2 times

Before you upgrade a Palo Alto Networks NGFW, what must you do?

- A. Make sure that the PAN-OS support contract is valid for at least another year.
- B. Export a device state of the firewall.
- C. Make sure that the firewall is running a supported version of the app + threat update.
- D. Make sure that the firewall is running a version of antivirus software and a version of WildFire that support the licensed subscriptions.

Correct Answer: C

  **Plato22** Highly Voted  2 years, 8 months ago

It is C:
Dependencies

Before you upgrade, make sure the firewall is running a version of app + threat (content version) that meets the minimum requirement of the new PAN-OS

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRrCAK>

upvoted 11 times

  **Marcy** Highly Voted  2 years, 8 months ago

It is C.

From the link:

Before you upgrade, make sure the firewall is running a version of app + threat (content version) that meets the minimum requirement of the new PAN-OS (see release notes). We recommend always running the latest version of content to ensure the most accurate and effective protections are being applied.

upvoted 7 times

  **TAKUM1y** Most Recent  1 year, 10 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/upgrade-pan-os/pan-os-upgrade-checklist#id53a2bc2b-f86e-4ee5-93d7-b06aff837a00>

"Verify the minimum content release version."



upvoted 2 times

  **rconway** 2 years, 5 months ago

Selected Answer: C

Apps and threats should be upgraded prior to upgrading the firewall.

upvoted 3 times

  **CG22** 2 years, 5 months ago

Selected Answer: C

it's C



upvoted 2 times

  **AbuHussain** 2 years, 5 months ago

Selected Answer: C

It is C.


upvoted 1 times

  **ev333** 2 years, 6 months ago

Selected Answer: C

I have run in to this while upgrading

upvoted 1 times

  **Plato22** 2 years, 8 months ago

Could also be C.

upvoted 2 times

The UDP-4501 protocol-port is used between which two GlobalProtect components?

- A. GlobalProtect app and GlobalProtect satellite
- B. GlobalProtect app and GlobalProtect portal
- C. GlobalProtect app and GlobalProtect gateway
- D. GlobalProtect portal and GlobalProtect gateway

Correct Answer: C

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/reference-port-number-usage/ports-used-for-globalprotect.html>

  **TAKUM1y** Highly Voted  1 year, 10 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/reference-port-number-usage/ports-used-for-globalprotect>

"Used for IPsec tunnel connections between GlobalProtect apps and gateways."



upvoted 5 times

  **Od2fdfa** Most Recent  3 months, 2 weeks ago

Selected Answer: C

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/firewall-administration/reference-port-number-usage/ports-used-for-globalprotect>

upvoted 1 times

  **Whizdhum** 8 months, 3 weeks ago

Answer is C. App-ID is paloalto-gp-mfa-notification. MultiFactor Authentication gateway (firewall) sends an UDP notification message to GlobalProtect client, when the client accesses a non-browser (such as SSH) based resource, to notify the client/end-user to authenticate first before accessing the resource.

upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: C

UDP 4501 is used for IPSEC and 443 for SSL-based tunnel

upvoted 2 times

  **prosto_marussia** 2 years, 7 months ago

Selected Answer: C

UDP 4501 Used for IPsec tunnel connections between GlobalProtect apps and gateways.

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/reference-port-number-usage/ports-used-for-globalprotect.html>

upvoted 3 times



An enterprise has a large Palo Alto Networks footprint that includes onsite firewalls and Prisma Access for mobile users, which is managed by Panorama. The enterprise already uses GlobalProtect with SAML authentication to obtain IP-to-user mapping information. However, Information Security wants to use this information in Prisma Access for policy enforcement based on group mapping. Information Security uses on-premises Active Directory (AD) but is uncertain about what is needed for Prisma Access to learn groups from AD. How can policies based on group mapping be learned and enforced in Prisma Access?

- A. Configure Prisma Access to learn group mapping via SAML assertion.
- B. Set up group mapping redistribution between an onsite Palo Alto Networks firewall and Prisma Access.
- C. Assign a master device in Panorama through which Prisma Access learns groups.
- D. Create a group mapping configuration that references an LDAP profile that points to on-premises domain controllers.

Correct Answer: C



Reference:

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/configure-user-based-policies-with-prisma-access/retrieve-user-id-information.html#id823f5b30-2c1d-4c87-9ae6-a06573455af7>

  **Whizdhum** 8 months, 3 weeks ago

Answer is C. Configure the Directory Sync component of the Cloud Identity Engine to retrieve user and group information from your Active Directory (AD); then, configure Group Mapping Settings in your Mobile Users—GlobalProtect, Mobile Users—Explicit Proxy, or remote network deployment. Alternatively, you can enable username-to-user group mapping for mobile users and users at remote networks using an LDAP server profile. The Cloud Identity Engine doesn't auto-populate groups to Panorama, so a master device or Cloud Identity Engine and specify it during the Prisma Access configuration. This answer assumes that the LDAP profile option is not used - Cloud Identity Engine is preferred.

upvoted 1 times



  **Kris92** 9 months, 1 week ago

Selected Answer: C

For Group Mapping in Prisma you need Directory Sync, Master Device is only optional, without it you need to specify the full distinguished name (DN) of the group.

So none of the options are correct, but if I would need to pick I would go for C.

upvoted 1 times

  **RoamingFo** 9 months, 2 weeks ago

Both C & D are part of the requirements for Group-Based access

on this document <https://docs.paloaltonetworks.com/prisma/prisma-access/3-2/prisma-access-panorama-admin/configure-user-based-policies-with-prisma-access/configure-user-id-in-prisma-access>

STEP 2 refers to D "for Prisma Access Nodes to get group mapping"

STEP 3 refers to C "For Panorama to get the list of groups"

Note Both can be replaced with the Cloud Identity Engine "Recommended"



upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

Selected Answer: C

C is the correct answer.



upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/configure-user-based-policies-with-prisma-access/retrieve-user-id-information#id823f5b30-2c1d-4c87-9ae6-a06573455af7>

upvoted 3 times

  **sujss** 1 year, 4 months ago

Relevant text from the link..

You can populate the groups to allow them to be selected in security policy rule drop-down lists by either configuring a next-generation firewall as a Master Device or configuring the Cloud Identity Engine to do so.

upvoted 1 times

  **nekkrovl** 2 years ago

D is correct too, you can use LDAP for Group Mapping in Prisma

upvoted 3 times

  **JMIB** 2 years ago

C is correct

Assign a master device in Panorama through which Prisma Access learns groups.

upvoted 1 times

  **prosto_marussia** 2 years, 7 months ago

Should be B.

1. Configure User-ID in Prisma Access
2. Configure User-ID for Remote Network Deployments
3. Configure Your Prisma Access Deployment to Retrieve Group Mapping
4. Redistribute User-ID Information Between Prisma Access and On-Premises Firewalls
5. Collect User and Group Information Using the Directory Sync Service

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/configure-user-based-policies-with-prisma-access>
upvoted 1 times

  **prosto_marussia** 2 years, 7 months ago

Ah, no. C is correct.

Above is relevant for USED-ID distribution, but for group mappings:

Step 3: Allow Panorama to use group mappings in security policies by configuring one or more next-generation on-premises or VM-series firewalls as a Master Device.

If you don't configure a Master Device with a Prisma Access User-ID deployment, use long-form distributed name (DN) entries instead.

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/configure-user-based-policies-with-prisma-access/configure-user-id-in-prisma-access.html>

upvoted 4 times

  **KKQQ12345** 2 years ago

Redistribution is for ip-user mapping, not group mapping.

upvoted 1 times

Question #237

Topic 1

What happens to traffic traversing SD-WAN fabric that doesn't match any SD-WAN policies?

- A. Traffic is dropped because there is no matching SD-WAN policy to direct traffic.
- B. Traffic matches a catch-all policy that is created through the SD-WAN plugin.
- C. Traffic matches implied policy rules and is redistributed round robin across SD-WAN links.
- D. Traffic is forwarded to the first physical interface participating in SD-WAN based on lowest interface number (i.e., Eth1/1 over Eth1/3).

Correct Answer: C

Reference:




<https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/configure-sd-wan/distribute-unmatched-sessions.html>

  **GivemeMoney** Highly Voted  2 years, 7 months ago

Selected Answer: C

C. Traffic matches implied policy rules and is redistributed round robin across SD-WAN links.

upvoted 6 times

  **TAKUM1y** Most Recent  1 year, 10 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/sd-wan/3-0/sd-wan-admin/configure-sd-wan/distribute-unmatched-sessions>

"If there is no match to any SD-WAN policy rule in the list, the session matches an implied SD-WAN policy rule at the end of the list that uses the round-robin method to distribute unmatched sessions among all links in one SD-WAN interface, which is based on the route lookup."

upvoted 4 times

  **Marcy** 2 years, 8 months ago

C is correct.

If there is no match to any SD-WAN policy rule in the list, the session matches an implied SD-WAN policy rule at the end of the list that uses the round-robin method to distribute unmatched sessions among all links in one SD-WAN interface, which is based on the route lookup.

upvoted 4 times

A remote administrator needs firewall access on an untrusted interface. Which two components are required on the firewall to configure certificate-based administrator authentication to the web UI? (Choose two.)

- A. certificate authority (CA) certificate
- B. server certificate
- C. client certificate
- D. certificate profile

Correct Answer: AD

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-administrative-accounts-and-authentication/configure-certificate-based-administrator-authentication-to-the-web-interface.html>

  **Marcy** Highly Voted 2 years, 8 months ago

Should be AD.

Generate a certificate authority (CA) certificate on the firewall.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-administrative-accounts-and-authentication/configure-certificate-based-administrator-authentication-to-the-web-interface.html>

upvoted 13 times

  **homersimpson** 2 years, 8 months ago

I agree, you create a cert profile, which specifies the CA cert to use. The client certs are all signed by the CA, so this makes the fw trust them.

upvoted 3 times

  **duckduckgoo** 1 year, 5 months ago

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-administrative-accounts-and-authentication/configure-certificate-based-administrator-authentication-to-the-web-interface>

upvoted 1 times

  **123XYZT** Most Recent 3 months, 1 week ago

A and D

Steps

Generate a certificate authority (CA) certificate on the firewall.

Configure a certificate profile for securing access to the web interface.

Configure the firewall to use the certificate profile for authenticating administrators.



Configure the administrator accounts to use client certificate authentication.

Generate a client certificate for each administrator.

Export the client certificate.

Import the client certificate into the client system of each administrator who will access the web interface.

upvoted 1 times

  **Whizdhum** 8 months, 3 weeks ago

Answers are A, D. As a more secure alternative to password-based authentication to the firewall web interface, you can configure certificate-based authentication for administrator accounts that are local to the firewall. Generate a certificate authority (CA) certificate on the firewall. You will use this CA certificate to sign the client certificate of each administrator. Configure a certificate profile for securing access to the web interface. Configure the firewall to use the certificate profile for authenticating administrators.

upvoted 1 times

  **Andromeda1800** 8 months, 3 weeks ago

Selected Answer: AD

Question asks "required on the firewall" so it's A and D. Client certificate is required to be on the client device, not on the firewall. Firewall needs to trust client certificate which needs to be assigned by a CA that firewall trusts, therefore CA root certificate needs to be imported to firewall.

upvoted 1 times

  **Andromeda1800** 8 months, 3 weeks ago

signed by a CA that firewall trusts... not assigned.

upvoted 1 times

  **Kalipso21** 1 year, 7 months ago

In the documentation:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/certificate-management/configure-an-sslts-service-profile>



It says: Use only signed certificates, not CA certificates, in SSL/TLS service profiles.

So I think it is C and D.

upvoted 2 times

  **DenskyDen** 1 year, 7 months ago

you don't need client certificate on the firewall, the question includes "two components are required on the firewall" should be A and D.
upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

AD.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-administrative-accounts-and-authentication/configure-certificate-based-administrator-authentication-to-the-web-interface#id3ec24be4-3aea-4ebd-8e2c-8928ae55fe53>

upvoted 1 times

  **AbuHussain** 2 years, 5 months ago

Selected Answer: AD

Should be AD.

upvoted 4 times

  **RamanJoshi** 2 years, 7 months ago

A and D, these two options are required on the firewall. Client certificate only needed on the client system and can be enterprise CA generated.
upvoted 1 times

  **GivemeMoney** 2 years, 7 months ago

Selected Answer: AD

A. certificate authority (CA) certificate
D. certificate profile

upvoted 3 times

  **drrealst** 2 years, 8 months ago

this is super confusion, C is kinda valid because you generate client certs for each user and is a step in the process.

upvoted 1 times

  **Jared28** 2 years, 5 months ago

The client cert doesn't go *on the firewall*. I think that's the key phrasing that makes AD most valid.

upvoted 2 times

  **Pretorian** 2 years ago

Great point, you are right...

upvoted 1 times

An administrator with 84 firewalls and Panorama does not see any WildFire logs in Panorama.
All 84 firewalls have an active WildFire subscription. On each firewall, WildFire logs are available.
This issue is occurring because forwarding of which type of logs from the firewalls to Panorama is missing?

- A. WildFire logs
- B. System logs
- C. Threat logs
- D. Traffic logs

Correct Answer: A

Reference:

<https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/manage-log-collection/configure-log-forwarding-to-panorama.html>

  **Bubu3k** Highly Voted 2 years, 4 months ago

It's C, threat logs

"Access to the WildFire logs from Panorama requires the following: a WildFire subscription, a File Blocking profile that is attached to a Security rule, and Threat log forwarding to Panorama."

<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/monitor-network-activity/use-case-respond-to-an-incident-using-panorama/review-wildfire-logs>

upvoted 12 times

  **poiuytr** 2 years, 4 months ago

Looks strange, but it's how it is written in documentation - answer "C"

upvoted 1 times

  **secdaddy** 1 year, 11 months ago

Confirmed still the same in 10.2 - updated URL link :

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/monitor-network-activity/use-case-respond-to-an-incident-using-panorama/review-wildfire-logs>

upvoted 1 times

  **Abu_Muhammad** Highly Voted 2 years, 4 months ago

Selected Answer: A

A is correct

upvoted 7 times



  **Od2fdfa** Most Recent 3 months, 2 weeks ago

Selected Answer: C

Access to the WildFire logs from Panorama requires the following: a WildFire subscription, a File Blocking profile that is attached to a Security rule, and Threat log forwarding to Panorama.

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/monitor-network-activity/use-case-respond-to-an-incident-using-panorama/review-wildfire-logs>

upvoted 1 times

  **46a6111** 5 months, 3 weeks ago

Selected Answer: C

Answer is C

upvoted 1 times

  **Thunnu** 6 months ago

Answer is A, read the question "This issue is occurring because forwarding of which type of logs FROM the firewalls to Panorama is missing?" So log forwarding config is firewall is missing.

upvoted 1 times

  **PietPompies_123** 6 months, 2 weeks ago

Jeepers is it A or C???

upvoted 1 times

  **scanossa** 7 months ago

Selected Answer: C


Access to the WildFire logs from Panorama requires the following: a WildFire subscription, a File Blocking profile that is attached to a Security rule, and Threat log forwarding to Panorama.

upvoted 1 times

[-]  **a9c4b5a** 7 months, 1 week ago

Selected Answer: C

C is correct
upvoted 1 times


[-]  **Whizdhum** 8 months, 3 weeks ago

Answer is C. Access to the WildFire logs from Panorama requires the following: a WildFire subscription, a File Blocking profile that is attached to a Security rule, and Threat log forwarding to Panorama.
upvoted 1 times

[-]  **Betty2022** 1 year, 1 month ago

Selected Answer: A

The real exam question will have better wording. Watch out for either Wildfire Submission logs, or Wildfire Virus entries.
A: would be for wildfire submission logs
C: would be for wildfire-virus logs
Based on this question, i go for A
upvoted 4 times

[-]  **KH29** 1 year, 2 months ago

Selected Answer: C

So "C" is correct the answer. If we want to view WildFire log on Panorama, required to have an active WildFire subscription and File blocking profile attached to security rule and configure threats logs to Panorama as well.

The questions is asking, which type of log are missing on Panorama? they didn't mention. about threat log has configure or not. Meaning, The threats log may not be configured.

Following official documentation: <https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/monitor-network-activity/use-case-respond-to-an-incident-using-panorama/review-wildfire-logs>

Regards, KH29
upvoted 1 times

[-]  **playthegamewithme** 1 year, 3 months ago

The correct answer is A, I have checked in my lab.
upvoted 2 times

[-]  **kewokil120** 1 year, 4 months ago

Selected Answer: C

Confirmed still the same in 10.2 - updated URL link :
<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/monitor-network-activity/use-case-respond-to-an-incident-using-panorama/review-wildfire-logs>
upvoted 1 times

[-]  **Pochex** 1 year, 5 months ago

Answer C
Based on the links provided in other comments, C is the correct answer, even if there is a log type called 'wildfire' in the Log Forwarding Profile.
upvoted 1 times

[-]  **Frightened_Acrobat** 1 year, 5 months ago

Selected Answer: A

The question asks, "forwarding of which type of logs" is missing from the firewalls? There is a type 'wildfire' in Log Forwarding profile separate from type 'threat.' So has to be A.
upvoted 5 times

[-]  **mic_mic** 1 year, 7 months ago

Access to the WildFire logs from Panorama requires the following: a WildFire subscription, a File Blocking profile that is attached to a Security rule, and Threat log forwarding to Panorama.
(<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/monitor-network-activity/use-case-respond-to-an-incident-using-panorama/review-wildfire-logs>)
In the NGFW go to: Objects > Log forwarding > add a log profile > log type Wildfire
<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/configure-log-forwarding>
On that page they talk about:
Create a Log Forwarding profile.
"The profile defines the destinations for Traffic, Threat, WildFire Submission, URL Filtering, Data Filtering, Tunnel and Authentication logs"
But if you check the config is called "WildFire" and not "WildFire Submission"
So you both right? Depends on which log you talking about.
upvoted 2 times

[-]  **dogeatdog** 1 year, 8 months ago

correction: #405. not #425
upvoted 1 times

A company wants to use their Active Directory groups to simplify their Security policy creation from Panorama. Which configuration is necessary to retrieve groups from Panorama?

- A. Configure an LDAP Server profile and enable the User-ID service on the management interface.
- B. Configure a group mapping profile to retrieve the groups in the target template.
- C. Configure a Data Redistribution Agent to receive IP User Mappings from User-ID agents.
- D. Configure a master device within the device groups.

Correct Answer: D

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PMtpCAG>

  **Gab99** Highly Voted 1 year, 6 months ago

Selected Answer: A


I am not sure what you are all relating to, but

.. AD groups are always gathered from LDAP(AD servers), so an LDAP profile must be distributed via template from Panorama. Each FW gets his groups then directly from LDAP.

The MASTER DEVICE is ONLY used for User-ID information gathering! Please take a look in Panorama Device groups, label says "master device is the firewall which Panorama gathers user ID info for use in policies". Nothing to do with groups here!

So answer CANNOT be D if the question is related to AD groups! Only A or B are possible.

upvoted 6 times


  **Jared28** 6 months, 1 week ago

Answer is C

Direct from Panorama, when you select a User ID Master device the check option for it specifies to store groups too.

"Store users and groups from Master Device if Reporting and Filtering on Groups is enabled in Panorama Settings"

upvoted 1 times

  **Jared28** 6 months, 1 week ago

Whoops, meant D, the answer is D

upvoted 1 times

  **123XYZT** Most Recent 3 months, 1 week ago

D

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PMtpCAG>


upvoted 1 times

  **scanossa** 7 months ago

Selected Answer: D

On the device group settings, you would have to select the master device from which Panorama would pull the users' information from

upvoted 1 times

  **Whizdhum** 8 months, 3 weeks ago

Answer is D. To simplify the creation or modification of user- and group-based policies, you can use a Master Device to add the group names to drop-down lists in security policy rules. You need to designate a firewall as a Master Device for each device group. After you add a Master Device, the device group inherits all policies defined on the master device; for this reason, it should be a standalone, dedicated device to be used for that device group. Alternatively, you can enable username-to-user group mapping using an LDAP profile with a Group Include List.

upvoted 1 times

  **Metgatz** 9 months ago

D is correct Option

upvoted 1 times

  **davidpm** 1 year ago

Selected Answer: D

D Correct

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PMtpCAG>

upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: D

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PMtpCAG>

upvoted 3 times

  **Alen** 2 years ago



as per everyones comments, the question needs to be re-worded. if groups are to be pulled from firewall, then D is correct

upvoted 1 times

  **JMIB** 2 years ago



D correct

upvoted 2 times

  **habeeb222** 2 years, 1 month ago

pulling from Panaroma* B - <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIIOCA0>



upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: D


D correct

upvoted 2 times

  **mtopolovec** 2 years, 2 months ago

This question is not formed right. It is asking about "retrieving groups from Panorama", but it should be about "Panorama retrieving groups from Firewall".

upvoted 2 times

  **DavidBackham2020** 2 years, 8 months ago

D is correct but you still need to get the group information on the master device (firewall) which I already configured as decried in A. Please note: You cannot configure A on Panorama.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIFQCA0>

I guess what I am trying to say: I don't like the question. But D seems to be the most correct answer, ignoring how the Group information is provided to the FW.

upvoted 4 times



How can packet buffer protection be configured?

- A. at zone level to protect firewall resources and ingress zones, but not at the device level
- B. at the interface level to protect firewall resources
- C. at the device level (globally) to protect firewall resources and ingress zones, but not at the zone level
- D. at the device level (globally) and, if enabled globally, at the zone level

Correct Answer: D

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/zone-protection-and-dos-protection/configure-zone-protection-to-increase-network-security/configure-packet-buffer-protection>

  **Marcy** Highly Voted 2 years, 8 months ago

D is correct.

You can configure Packet Buffer Protection at two levels: the device level (global) and if enabled globally, you can also enable it at the zone level

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/zone-protection-and-dos-protection/configure-zone-protection-to-increase-network-security/configure-packet-buffer-protection.html>

upvoted 12 times

  **procheeseburger** Most Recent 1 year, 2 months ago

This is a practice Question, wont be on the test.

upvoted 1 times

  **TAKUM1y** 1 year, 9 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/packet-buffer-protection>

upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/configure-zone-protection-to-increase-network-security/configure-packet-buffer-protection>

"You can configure Packet Buffer Protection at two levels: the device level (global) and if enabled globally, you can also enable it at the zone level."

upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: D

D according to:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/configure-zone-protection-to-increase-network-security/configure-packet-buffer-protection>

You can configure Packet Buffer Protection at two levels: the device level (global) and if enabled globally, you can also enable it at the zone level. Global packet buffer protection (Device->Setup->Session) is to protect firewall resources and ensure that malicious traffic does not cause the firewall to become non-responsive.

Packet buffer protection per ingress zone (Network->Zones) is a second layer of protection that starts blocking the offending IP address if it continues to exceed the packet buffer protection thresholds.

The most effective way to block DoS attacks against a service behind the firewall is to configure packet buffer protection globally and per ingress zone.

You can Enable Packet Buffer Protection for a zone, but it is not active until you enable packet buffer protection globally and specify the settings.

upvoted 4 times



An existing NGFW customer requires direct internet access offload locally at each site, and IPSec connectivity to all branches over public internet. One requirement is that no new SD-WAN hardware be introduced to the environment. What is the best solution for the customer?

- A. Configure a remote network on PAN-OS
- B. Upgrade to a PAN-OS SD-WAN subscription
- C. Configure policy-based forwarding
- D. Deploy Prisma SD-WAN with Prisma Access

Correct Answer: B

Reference:

<https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/about-sd-wan.html>

  **Whizdhum** 8 months, 3 weeks ago


Answer is C. Clearly, this is a question about SD-WAN, although the question isn't written well, we can still deduce the answer. SD-WAN is the best option. No additional hardware needed, just an SD-WAN subscription. You may have cloud-based services and instead of having your internet traffic flow from branches to the hub to the cloud, you want the internet traffic to flow directly from branches to the cloud using a directly connected ISP. Such access from a branch to the internet is Direct Internet Access (DIA). Use DIA on branches for SaaS, web browsing, or heavy-bandwidth applications that shouldn't be backhauled to a hub. This ties to the mention of "offloading" at each site.

upvoted 1 times

  **Metgatz** 9 months ago

B is correct option



upvoted 1 times

  **gc999** 10 months, 1 week ago

Selected Answer: C

The question asked "What is the best solution for customer". The best solution should be no need to do any upgrade or subscription. Besides, the requirement does not need any intelligent or dynamic path selection. So PBF is the best solution I think.

upvoted 2 times

  **DenskyDen** 1 year, 7 months ago

B. The PAN-OS software now includes a native SD-WAN subscription to provide intelligent and dynamic path selection on top of the industry-leading security that PAN-OS software already delivers. Key features of the SD-WAN implementation include centralized configuration management, automatic VPN topology creation, traffic distribution, monitoring, and troubleshooting.

<https://docs.paloaltonetworks.com/sd-wan>

upvoted 3 times

  **mz101** 1 year, 9 months ago

B is fine, but anything wrong with C, using PBF?

upvoted 3 times

  **Pretorian** 2 years ago

Selected Answer: B

There are two SD-WAN options:

- Pan-OS SD-WAN which requires a subscription and leverages existing firewalls
- Cloudgenix SD-WAN which requires ION devices (hardware)

upvoted 3 times

A firewall administrator requires an A/P HA pair to fail over more quickly due to critical business application uptime requirements. What is the correct setting?

- A. Change the HA timer profile to "user-defined" and manually set the timers.
- B. Change the HA timer profile to "fast".
- C. Change the HA timer profile to "aggressive" or customize the settings in advanced profile.
- D. Change the HA timer profile to "quick" and customize in advanced profile.

Correct Answer: C

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/high-availability/set-up-activepassive-ha/configure-activepassive-ha.html>

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/set-up-activepassive-ha/configure-activepassive-ha>
upvoted 3 times

  **UFanat** 2 years, 2 months ago

Selected Answer: C

C is correct.
upvoted 2 times

  **prosto_marussia** 2 years, 7 months ago

Selected Answer: C

C is correct.

Use the Recommended profile for typical failover timer settings and the Aggressive profile for faster failover timer settings. The Advanced profile allows you to customize the timer values to suit your network requirements.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/high-availability/ha-concepts/ha-timers.html>
upvoted 4 times

What is the function of a service route?

- A. The service packets exit the firewall on the port assigned for the external service. The server sends its response to the configured source interface and source IP address.
- B. The service packets enter the firewall on the port assigned from the external service. The server sends its response to the configured destination interface and destination IP address.
- C. The service route is the method required to use the firewall's management plane to provide services to applications.
- D. Service routes provide access to external services, such as DNS servers, external authentication servers or Palo Alto Networks services like the Customer Support Portal.

Correct Answer: A

Reference:



<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/service-routes.html>

  **west33637** Highly Voted 1 year, 10 months ago

Selected Answer: D

The answer is D. They asked what is the function? Not how does it work. But, what is the function. (A) does not describe the function. Look at the documentation, "The firewall uses the management (MGT) interface by default to access external services, such as DNS servers, external authentication servers, Palo Alto Networks® services such as software, URL updates, licenses and AutoFocus. An ALTERNATIVE to using the MGT interface is to configure a data port (a regular interface) to access these services." -<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/service-routes/service-routes-overview#id69ef535a-d5b0-4c79-bb7f-1302a438e7c5>

upvoted 20 times

  **Eluis007** 4 months, 4 weeks ago

Why do you ignore this "Customer Support Portal"? How can service routes be used to "provide access to CSP"???

upvoted 1 times

  **jeremykebir** Most Recent 2 months, 1 week ago

For the peoples who have still doubt about the answer it should be D.


What is the function of a service route?

A. The service packets exit the firewall on the port assigned for the external service. The server sends its response to the configured source interface and source IP address.

D. Service routes provide access to external services, such as DNS servers, external authentication servers or Palo Alto Networks services like the Customer Support Portal.

The question is about "service routes" and no "service packet" in the answer A that doesn't exist :D

upvoted 1 times



  **Od2fdfa** 3 months, 2 weeks ago

Option A is correct

Below option is wrong because although service routes provide access to external services but they are not configured by default. They are to be used in case management interface is not to be used.

D. Service routes provide access to external services, such as DNS servers, external authentication servers or Palo Alto Networks services like the Customer Support Portal.

upvoted 1 times

  **Od2fdfa** 3 months, 2 weeks ago

Actually just ignore that. The correct option is D because the question is about the "Function"

Option A is not a function.

D seems to be a more specific response to the question.

upvoted 1 times

  **Thunnu** 6 months ago

Answer is A

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/service-routes/service-routes-overview#id69ef535a-d5b0-4c79-bb7f-1302a438e7c5>

upvoted 1 times

  **Xuzi** 9 months, 3 weeks ago

The service packets exit the firewall on the port assigned for the external service and the server sends its response to the configured source interface and source IP address.

upvoted 1 times

sov4 1 year, 1 month ago

Selected Answer: A

It's A. D almost got me except you dont access the Customer Support Portal via a service route. That's via a web browser smh.
upvoted 3 times

mercysayno765 1 year, 1 month ago

Selected Answer: A

First Paragraph, Last statement
"The service packets exit the firewall on the port assigned for the external service and the server sends its response to the configured source interface and source IP address."

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/service-routes/service-routes-overview#id69ef535a-d5b0-4c79-bb7f-1302a438e7c5>

upvoted 4 times

Pochex 1 year, 5 months ago

Answer A

I can access the CSP even though I have no firewall in use. D is not the correct one.

upvoted 3 times

lildevil 1 year, 3 months ago

The answer D does say "Like the customer support portal" doesn't say it's the only thing...and the FW does contact that for license and if the case maybe ZTP for device certificate. Having said that answer A definitely comes verbatim from the documentation. Both are seemingly accurate.

upvoted 1 times

Frightened_Acrobat 1 year, 5 months ago

Selected Answer: A

Trick question. D lists Customer Support Portal at the end. This is not a function of Service Routes. D cannot be correct.

upvoted 3 times

[Removed] 1 year, 5 months ago

Selected Answer: D

function not how it works

upvoted 1 times

zemijan 1 year, 6 months ago

Is D. The firewall uses the management (MGT) interface by default to access external services, such as DNS servers, external authentication servers ...

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/service-routes>

upvoted 1 times

mic_mic 1 year, 7 months ago

Selected Answer: A

In the real exam the answer is: Service route defines the source interface which must used by the firewall when generating the specific traffic

upvoted 1 times

TAKUM1y 1 year, 10 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/service-routes/service-routes-overview#id69ef535a-d5b0-4c79-bb7f-1302a438e7c5>

upvoted 1 times

mysteryjoker 1 year, 10 months ago

answer is A, not D. You don' t need a service route to access the support portal you just access via a browser.

upvoted 2 times

UFanat 2 years, 2 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/service-routes/service-routes-overview#id69ef535a-d5b0-4c79-bb7f-1302a438e7c5>

"The service packets exit the firewall on the port assigned for the external service and the server sends its response to the configured source interface and source IP address."

upvoted 3 times

NLT 2 years, 6 months ago

The firewall uses the management (MGT) interface by default to access external services, such as DNS servers, external authentication servers, Palo Alto Networks services such as software, URL updates, licenses and AutoFocus. An alternative to using the MGT interface is to configure a data port (a regular interface) to access these services. The path from the interface to the service on a server is known as a service route. The service packets exit the firewall on the port assigned for the external service and the server sends its response to the configured source interface and source IP address.

upvoted 1 times

GivemeMoney 2 years, 7 months ago

Selected Answer: A

A is correct.

upvoted 3 times

DRAG DROP -

Place the steps to onboard a ZTP firewall into Panorama/CSP/ZTP-Service in the correct order.

Select and Place:

- Installer or IT administrator registers ZTP firewalls by adding them to Panorama using firewall serial number and claim key.
- After connecting to the internet, the ZTP firewall requests a device certificate from the CSP in order to connect to the ZTP service.
- The ZTP firewalls connect to Panorama and the device group and template configurations are pushed from Panorama to the ZTP firewalls.
- The ZTP service pushes the Panorama IP or FQDN to the ZTP firewalls.
- Panorama registers the firewalls with the CSP. After the firewalls are successfully registered, the firewall is associated with the same ZTP tenant as the Panorama in the ZTP service.

Answer Area

-
-
-
-
-

FIRST

SECOND

THIRD

FOURTH

FIFTH

Correct Answer:

-
-
-
-
-

Answer Area

- Installer or IT administrator registers ZTP firewalls by adding them to Panorama using firewall serial number and claim key.
- Panorama registers the firewalls with the CSP. After the firewalls are successfully registered, the firewall is associated with the same ZTP tenant as the Panorama in the ZTP service.
- After connecting to the internet, the ZTP firewall requests a device certificate from the CSP in order to connect to the ZTP service.
- The ZTP service pushes the Panorama IP or FQDN to the ZTP firewalls.
- The ZTP firewalls connect to Panorama and the device group and template configurations are pushed from Panorama to the ZTP firewalls.

FIRST

SECOND

THIRD

FOURTH

FIFTH

Reference:

<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/set-up-zero-touch-provisioning/ztp-overview/ztp-configuration-elements.html>

 **Marcy** Highly Voted 2 years, 8 months ago
Verified correct.

<https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/manage-firewalls/set-up-zero-touch-provisioning/ztp-overview/ztp-configuration-elements.html>
upvoted 7 times

DenskyDen Most Recent 1 year, 7 months ago

Installer or IT administrator registers ZTP firewalls by adding them to Panorama using the firewall serial number and claim key. Panorama registers the firewalls with the CSP. After the firewalls are successfully registered, the firewall is associated with the same ZTP tenant as the Panorama in the ZTP service. ZTP firewalls successfully registered with the ZTP service are automatically added as managed firewalls (PanoramaManaged Devices) on Panorama. When the firewall connects to the Internet, the ZTP firewall requests a device certificate from the CSP in order to connect to the ZTP service. The ZTP service pushes the Panorama IP or FQDN to the ZTP firewalls. The ZTP firewalls connect to Panorama and the device group and template configurations are pushed from Panorama to the ZTP firewalls.
upvoted 2 times

TAKUM1y 1 year, 10 months ago

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/set-up-zero-touch-provisioning/ztp-overview/ztp-configuration-elements>
upvoted 3 times

Toeknee76 2 years, 1 month ago

No Images in this question.... This is my angry face.....
upvoted 1 times

Question #246

Topic 1

Which of the following commands would you use to check the total number of the sessions that are currently going through SSL Decryption processing?

- A. show session all filter ssl-decryption yes total-count yes
- B. show session all ssl-decrypt yes count yes
- C. show session all filter ssl-decrypt yes count yes
- D. show session filter ssl-decryption yes total-count yes

Correct Answer: C

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIF2CAK>

Marcy Highly Voted 2 years, 8 months ago

C is correct.
upvoted 7 times

GivemeMoney Highly Voted 2 years, 7 months ago

Selected Answer: C

To display the count of decrypted sessions

> show session all filter ssl-decrypt yes count yes

Number of sessions that match filter: 2758
upvoted 5 times

DenskyDen Most Recent 1 year, 7 months ago

Definitely C.
upvoted 1 times

TAKUM1y 1 year, 10 months ago

Selected Answer: C

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIF2CAK>
upvoted 1 times

Template Stack ?

Name

Default VSYS v

The default virtual system template configuration is pushed to firewalls with a single virtual system.

Description

<input type="checkbox"/>	TEMPLATES
<input type="checkbox"/>	Global
<input type="checkbox"/>	NYCFW
+ Add - Delete ↑ Move Up ↓ Move Down	

Refer to the image. An administrator is tasked with correcting an NTP service configuration for firewalls that cannot use the Global template NTP servers. The administrator needs to change the IP address to a preferable server for this template stack but cannot impact other template stacks. How can the issue be corrected?

- A. Override the value on the NYCFW template.
- B. Override a template value using a template stack variable.
- C. Override the value on the Global template.
- D. Enable "objects defined in ancestors will take higher precedence" under Panorama settings.

Correct Answer: B

Reference:

<https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/templates-and-template-stacks>

TAKUM1y Highly Voted 1 year, 10 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/templates-and-template-stacks>
upvoted 5 times

duckduckgoo 1 year, 5 months ago

I found another one that might help more.

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/configure-template-or-template-stack-variables>
upvoted 1 times

Whizdhum Most Recent 8 months, 3 weeks ago

Answer is B. There are two ways to override values pushed from a template or template stack. The first is to define a value locally on the firewall to override a value pushed from a template or template stack. The second is to define firewall-specific variables to override values pushed from a template or template stack.

upvoted 1 times

UTF 1 year, 4 months ago

B: This exact scenario is at the end of the 1st paragraph. With the actions to accomplish (2 ways) in the bullets below the info box.

<https://docs.paloaltonetworks.com/panorama/11-0/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/override-a-template-setting>
upvoted 2 times

awtsuriticuna 1 year, 9 months ago

Option B

Create a template or template stack variable to replace IP addresses, Group IDs, and interfaces in your configurations. Template variables are inherited by the template stack and you can override them to create a template stack variable

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/templates-and-template-stacks>

upvoted 3 times

While troubleshooting an SSL Forward Proxy decryption issue, which PAN-OS CLI command would you use to check the details of the end entity certificate that is signed by the Forward Trust Certificate or Forward Untrust Certificate?

- A. show system setting ssl-decrypt certs
- B. show system setting ssl-decrypt certificate
- C. debug dataplane show ssl-decrypt ssl-stats
- D. show system setting ssl-decrypt certificate-cache

Correct Answer: B

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000C1F2CAK>

  **UFanat** Highly Voted  2 years, 2 months ago

Selected Answer: B

```
> show system setting ssl-decrypt certificate
```

```
Certificates for Global
```

```
SSL Decryption CERT
```

```
global trusted
```

```
ssl-decryption x509 certificate
```

```
version 2
```

```
cert algorithm 4
```

```
valid 200502004326Z -- 300502005326Z
```

```
cert pki 1
```

```
subject: NAME
```

```
issuer: NAME
```

```
serial number(16)
```

```
60 c9 5....."
```

```
rsa key size 4096 bits siglen 512 bytes
```

```
basic constraints extension CA 1
```

```
global untrusted
```

```
ssl-decryption x509 certificate
```

```
version 2
```

```
cert algorithm 4
```

```
valid 200221032Z -- 220500032Z
```

```
cert pki 1
```

```
subject: untrust.xxx.net
```

```
issuer: untrust.xxx.net
```

```
serial number(9)
```

```
00 b8 db 95 e3 b0 f9 .....
```

```
rsa key size 2048 bits siglen 256 bytes
```

```
basic constraints extension CA 1
```

```
NO INBOUND CERT
```

```
> show system setting ssl-decrypt certificate-cache
```

```
Cached 0 certificates
```

```
upvoted 6 times
```

  **kacper_n99** Most Recent  3 months, 4 weeks ago

Selected Answer: D

Checked in the lab.



upvoted 1 times

  **Eluis007** 4 months, 4 weeks ago

Selected Answer: D

Checked in the lab

upvoted 1 times

  **Whizdhum** 8 months, 3 weeks ago

Selected Answer: D

Answer is D. The cache space is limited, so you will only see recent certificates cached if you have a busy firewall. But the certificates in that certificate cache are placed there when the firewall retrieves the certificate for a traffic flow that matches an SSL Forward Proxy decryption policy. Note that the end-entity certificate is the final link in the chain of trust.

upvoted 1 times

  **Whizdhum** 8 months, 3 weeks ago

Answer is D. The cache space is limited, so you will only see recent certificates cached if you have a busy firewall. But the certificates in that certificate cache are placed there when the firewall retrieves the certificate for a traffic flow that matches an SSL Forward Proxy decryption policy. Note that the end-entity certificate is the final link in the chain of trust.

upvoted 1 times

  **nguyendtv50** 1 year, 3 months ago

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIF2CAK>

upvoted 1 times

  **ConfuzedOne** 1 year, 3 months ago

Selected Answer: D

Read the question - "end entity certificate".
Now run the various command options on your firewall.

Answer A is invalid syntax

Answer B shows you your Certificates installed on your Palo; not end-entity certificates

Answer C shows you some various hit counters.

Answer D shows you certificate details from "end entities"

upvoted 3 times

  **tomsui44** 1 year, 3 months ago

Selected Answer: B

B. show system setting ssl-decrypt certificate

upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

B. just tested it.

upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: B

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIF2CAK>



upvoted 2 times

  **ManKing36** 2 years, 3 months ago

Selected Answer: D

Verified in lab - correct answer should be D

upvoted 1 times

  **UFanat** 2 years, 2 months ago

No, it's wrong.

> show system setting ssl-decrypt certificate-cache

Cached 0 certificates

upvoted 1 times

  **shinichi_88** 2 years, 7 months ago

B should be correct

upvoted 2 times

Which action disables Zero Touch Provisioning (ZTP) functionality on a ZTP firewall during the onboarding process?

- A. removing the Panorama serial number from the ZTP service
- B. performing a factory reset of the firewall
- C. performing a local firewall commit
- D. removing the firewall as a managed device in Panorama

Correct Answer: C

Reference:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000001UiOCAU&lang=en_US%E2%80%A9&refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail

  **dashiawia** Highly Voted 2 years, 8 months ago

C is the right answer.

<https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/manage-firewalls/set-up-zero-touch-provisioning/add-ztp-firewalls-to-panorama/add-a-ztp-firewall-to-panorama.html#id182211ac-a31c-4122-a11f-19450ec9ca4e>

upvoted 10 times

  **Marcy** 2 years, 8 months ago

You are correct. In your link:

Performing a local commit on the ZTP firewall disables ZTP functionality and results in the failure to successfully add the firewall to Panorama.

upvoted 4 times

  **Whizdhum** Most Recent 8 months, 3 weeks ago

Selected Answer: C

While adding ZTP firewalls to Panorama, do not perform any commits on the ZTP firewall before you verify that the firewall is successfully added to Panorama in Step 4. Performing a local commit on the ZTP firewall disables ZTP functionality and results in the failure to successfully add the firewall to Panorama.

upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/set-up-zero-touch-provisioning/add-ztp-firewalls-to-panorama/add-a-ztp-firewall-to-panorama>

"Performing a local commit on the ZTP firewall disables ZTP functionality and results in the failure to successfully add the firewall to Panorama."

upvoted 3 times

  **UFanat** 2 years, 2 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/manage-firewalls/set-up-zero-touch-provisioning/add-ztp-firewalls-to-panorama/add-a-ztp-firewall-to-panorama>

While adding ZTP firewalls to Panorama, do not perform any commits on the ZTP firewall before you verify that the firewall is successfully added to Panorama in Step 4. Performing a local commit on the ZTP firewall disables ZTP functionality and results in the failure to successfully add the firewall to Panorama.

upvoted 2 times



  **Loloshikovich** 2 years, 4 months ago

Selected Answer: C

Correct answer is C:

While adding ZTP firewalls to Panorama, do not perform any commits on the ZTP firewall before you verify that the firewall is successfully added to Panorama in Step 4. Performing a local commit on the ZTP firewall disables ZTP functionality and results in the failure to successfully add the firewall to Panorama.

upvoted 2 times

  **NLT** 2 years, 6 months ago

While adding ZTP firewalls to Panorama, do not perform any commits on the ZTP firewall before you verify that the firewall is successfully added to Panorama in Step 4. Performing a local commit on the ZTP firewall disables ZTP functionality and results in the failure to successfully add the firewall to Panorama.

upvoted 1 times

  **GivemeMoney** 2 years, 7 months ago

Selected Answer: C

dashiawia is correct - C is right!

upvoted 3 times

  **[Removed]** 2 years, 8 months ago

A. removing the Panorama serial number from the ZTP service

Delete a ZTP firewall from the list of firewalls for future registration with the ZTP service.

> request plugins ztp firewall-delete firewall <serial number>

<https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/manage-firewalls/set-up-zero-touch-provisioning/use-the-cli-for-ztp-tasks.html>

upvoted 1 times

  **zicouille** 2 years, 8 months ago

So it's C or D? looks like D for me?

upvoted 1 times

  **Mucho9999** 2 years, 8 months ago

Selected Answer: D

D <https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/manage-firewalls/set-up-zero-touch-provisioning/use-the-cli-for-ztp-tasks.html>

upvoted 2 times

  **Micutzu** 2 years, 8 months ago

Check also question #245.

Performing a local commit it's not part of the onboarding process.

upvoted 2 times

  **Mucho9999** 2 years, 8 months ago

I take it back its C :)

upvoted 2 times

  **RJ45TP** 2 years, 8 months ago

I think it is C because you have to do a commit after you run request disable-ztp

upvoted 2 times

  **Mucho9999** 2 years, 8 months ago

You do have to do a commit but the answer is too vague to be "correct enough"

upvoted 2 times

  **Marcy** 2 years, 8 months ago

I am having trouble finding the answer for this one. But I don't think it's C.

upvoted 2 times

  **GivemeMoney** 2 years, 7 months ago

But it is C, you said it was C up above.

upvoted 1 times

In URL filtering, which component matches URL patterns?

- A. live URL feeds on the management plane
- B. security processing on the data plane
- C. single-pass pattern matching on the data plane
- D. signature matching on the data plane

Correct Answer: C

Reference:

<https://www.firewall.cx/networking-topics/firewalls/palo-alto-firewalls/1152-palo-alto-firewall-single-pass-parallel-processing-hardware-architecture.html>

GBD35055 Highly Voted 1 year, 11 months ago

According to the PCNSE study guide page 75, URL match is part of Security Processing
upvoted 7 times

Pretorian Highly Voted 2 years ago

Selected Answer: B

Malicious question.

I'm gonna go with "B" because URL Filtering is NOT pattern based, this is one of the APP-ID components "Pattern based application identification".
upvoted 5 times

Raaf_NL Most Recent 7 months, 3 weeks ago

Selected Answer: C

Palo Alto Networks firewalls use a single-pass architecture, including single-pass pattern matching on the data plane, to efficiently process and inspect network traffic, including URL filtering. During this single-pass, the firewall inspects the content of the traffic for various security aspects, including URL patterns for URL filtering.
upvoted 1 times

Whizdhum 8 months, 3 weeks ago

Selected Answer: C

SP3 scans the contents based on the same stream and it uses uniform signature matching patterns to detect and block threats.
upvoted 1 times

Andromeda1800 8 months, 3 weeks ago

Selected Answer: B

URL is matched by security processing on the data plane. Security processing handles App-ID, User-ID, URL match, policy match, SSL/IPsec, decompression.

Signature match processing handles all the Threat prevention related operations/signature matching such as signature matching for exploits (vulnerability), virus, spyware plus credit card number, social security numbers. Signature matching component is capable of single-pass pattern match.

Both security processing and signature matching components are data plane components.
upvoted 1 times

wallaka 9 months, 1 week ago

Selected Answer: C

I'd say B, but the marketing phrase is usually the correct answer.
upvoted 1 times

droide 1 year, 6 months ago

Selected Answer: B

It's B.
You can see on this image (URL Match is part of security processing) :
http://3.bp.blogspot.com/-AXK7gc4JLe4/VUkMgHr6g_I/AAAAAAAASHs/DtAddpYvWJQ/s640/PA2.jpg
upvoted 3 times

hcir 2 months ago

in EDU-210, there is a similar slide that includes single pass in the pattern matching processor. So B.
upvoted 1 times

DenskyDen 1 year, 7 months ago

C. PA uses single pass architecture. One of the key elements to the single pass architecture is summed up accurately and succinctly with the phrase "scan it all, scan it once".

upvoted 2 times

  **mic_mic** 1 year, 7 months ago

Selected Answer: B

Agree on B, Yes it is part of the Single Pass Software Architecture, but no, it is not a pattern


upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: C

https://media.paloaltonetworks.com/documents/Single_Pass_Parallel_Processing_Architecture.pdf

upvoted 2 times

  **Aaronyukin** 1 year, 10 months ago

Selected Answer: B

The answer is B.

upvoted 3 times

  **kabobmyopic0h** 2 years, 3 months ago

The answer is B

The question is asking for which "Component" matches "URL" patterns?
URL matching happens at "security processing on the data plane"

Source: PCNSA Study Guide "illustration depicts the architecture of a Palo Alto Networks Next-Generation Firewall."

upvoted 4 times

  **bartbernini** 2 years, 6 months ago

Selected Answer: C

The correct answer is C.

"Palo Alto Networks Single Pass Software Architecture

...

Content-ID: a single hardware-accelerated signature matching engine that uses a uniform signature format to scan traffic for data (credit card numbers, social security numbers, and custom patterns) and threats (vulnerability exploits – IPS, viruses, and spyware) plus a URL categorization engine to perform URL filtering. "

https://media.paloaltonetworks.com/documents/Single_Pass_Parallel_Processing_Architecture.pdf

upvoted 3 times

In a template, you can configure which two objects? (Choose two.)

- A. Monitor profile
- B. application group
- C. SD-WAN path quality profile
- D. IPsec tunnel


Correct Answer: AD

  **Marcy** Highly Voted 2 years, 8 months ago

It is AD.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/network/network-network-profiles/network-network-profiles-monitor.html>

upvoted 13 times

  **Whizdhum** Most Recent 8 months, 3 weeks ago

Selected Answer: AD

Answers are A, D. Through the Device and Network tabs, you can deploy a common base configuration to multiple firewalls that require similar settings using a template or a template stack (a combination of templates). Essentially, if it exists under the Device or Network tabs, it can be used in a template.



upvoted 1 times

  **JMIB** 2 years ago

It is AD.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/network/network-network-profiles/network-network-profiles-monitor.html>

upvoted 1 times

  **renzanjo** 1 year, 11 months ago

Did anyone here passed the exam using examtopics? Planning to take this month.

upvoted 2 times

  **duckduckgoo** 1 year, 5 months ago

How did you do?

upvoted 1 times

  **UFanat** 2 years, 2 months ago

Selected Answer: AD

Application group and SD-WAN path quality profile should be configured in Objects tab which means in Device Group, not in a Template. Monitor Profile and IPsec tunnel are belong to Network tab (templates)

upvoted 4 times

  **confusion** 2 years, 4 months ago

Selected Answer: AD

AD - Templates / Network
BC - Device Groups / Objects

upvoted 2 times

  **Abu_Muhammad** 2 years, 4 months ago

Selected Answer: AD

A&D
others are under objects

upvoted 1 times

  **rconway** 2 years, 5 months ago

Selected Answer: AD

A and D are setup in the template.

upvoted 1 times

  **AbuHussain** 2 years, 5 months ago

A and D is correct

upvoted 1 times

[-] 👤 **king04** 2 years, 6 months ago

Selected Answer: AD

A and D is correct
upvoted 1 times

[-] 👤 **ev333** 2 years, 6 months ago

Selected Answer: AD

both are the domain of templates
upvoted 1 times

[-] 👤 **homersimpson** 2 years, 8 months ago

A+D are under templates. This is the answer.
B+C are under "Objects" tab, which is in Device Groups.
upvoted 2 times

[-] 👤 **yziyi** 2 years, 8 months ago

A & D !
upvoted 3 times

[-] 👤 **Bryan1151** 2 years, 8 months ago

A and D, just checked it on my firewall.
upvoted 2 times

[-] 👤 **Micutzu** 2 years, 8 months ago

AD are correct choices.
upvoted 4 times

[-] 👤 **kktan** 2 years, 8 months ago

Selected Answer: CD

application group under device group
upvoted 1 times

[-] 👤 **Marcy** 2 years, 8 months ago

SD-WAN path quality profile - also under device group
upvoted 3 times

[-] 👤 **Plato22** 2 years, 8 months ago

C and D are the correct answers.
A and B are part of device-groups.
upvoted 3 times

[-] 👤 **Mmiri** 11 months, 1 week ago

really?
upvoted 1 times

An organization's administrator has the funds available to purchase more firewalls to increase the organization's security posture. The partner SE recommends placing the firewalls as close as possible to the resources that they protect. Is the SE's advice correct, and why or why not?

- A. No. Firewalls provide new defense and resilience to prevent attackers at every stage of the cyberattack lifecycle, independent of placement.
- B. Yes. Firewalls are session-based, so they do not scale to millions of CPS.
- C. No. Placing firewalls in front of perimeter DDoS devices provides greater protection for sensitive devices inside the network.
- D. Yes. Zone Protection profiles can be tailored to the resources that they protect via the configuration of specific device types and operating systems.



Correct Answer: B

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/zone-protection-and-dos-protection.html>

  **Micutzu** Highly Voted 2 years, 8 months ago

I believe A is correct.
upvoted 9 times



  **joquin0020** 7 months ago

SO DO I
upvoted 1 times

  **TAKUM1y** Highly Voted 1 year, 10 months ago



Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/firewall-placement-for-dos-protection>
"The firewall is a session-based device that isn't designed to scale to millions of connections-per-second (CPS) to defend against large volumetric DoS attacks"
upvoted 6 times

  **Whizdhum** Most Recent 8 months, 3 weeks ago

Selected Answer: B



Answer is B. The firewall is a session-based device that isn't designed to scale to millions of connections-per-second (CPS) to defend against large volumetric DoS attacks. For the best DoS protection, place firewalls as close to the resources you're protecting as possible. This reduces the number of sessions the firewall needs to handle and therefore the amount of firewall resources required to provide DoS protection.
upvoted 2 times

  **gc999** 10 months, 1 week ago

Selected Answer: D

I will choose D. The question said "purchase more firewall", but not "purchase a higher ended model firewall". Multiple Firewalls put on the core network? How can it be connected? If for "more" firewalls which run the same security posture, it should be put as closes as the resources (i.e. servers sides). So it must be "Yes". Then Firewalls are session-based and it is truth, then so?

"D" should be more correct so it can define specific security policy for the specific protected resource.
upvoted 1 times

  **Sarbi** 1 year, 8 months ago

B is correct always place firewalls behind high-volume devices.
upvoted 2 times

  **Khs01** 2 years ago

Selected Answer: B

Definitevely B
upvoted 2 times

  **UFanat** 2 years, 2 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/firewall-placement-for-dos-protection>
upvoted 2 times

  **Abu_Muhammad** 2 years, 4 months ago

Selected Answer: B

B
This was mentioned in PBP section
upvoted 2 times

[-] 👤 **Loloshikovichev** 2 years, 4 months ago

Answers make no sense. Yes firewall should be closer in terms of DDoS protection. But palo has firewalls with up to 4 million CPS, so answer B is not the correct one as firewalls can scale to millions of CPS. Answer D makes no sense as well, what kind of tailoring to operating systems?
upvoted 1 times

[-] 👤 **secdaddy** 1 year, 11 months ago

Choose the least bad answer then, which is B. The fewer sessions a firewall will need to handle (ie because it's behind a DDOS screen or because routing of flows to other parts of the network reduces the flows going across this firewall towards the specific protected resources) the less the customer needs to spend on the hardware.
upvoted 1 times

[-] 👤 **mikecorleone88** 2 years, 5 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/firewall-placement-for-dos-protection>
upvoted 2 times

[-] 👤 **Mp84047** 2 years, 5 months ago

B is the correct answer

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/firewall-placement-for-dos-protection>
upvoted 1 times

[-] 👤 **john_smith** 2 years, 7 months ago

Why not B?

"The firewall is a session-based device that isn't designed to scale to millions of connections-per-second (CPS) to defend against large volumetric DoS attacks."

"For the best DoS protection, place firewalls as close to the resources you're protecting as possible. This reduces the number of sessions the firewall needs to handle and therefore the amount of firewall resources required to provide DoS protection."

upvoted 3 times

[-] 👤 **prosto_marussia** 2 years, 7 months ago

Agree with D.

upvoted 1 times

[-] 👤 **GivemeMoney** 2 years, 7 months ago

D

interesting they used the word "Firewalls" in the other three answers, and in the answer linked documented the word "Tailor" is used, which reads more like subconscious marketing.

upvoted 1 times

[-] 👤 **ericksc9514** 2 years, 7 months ago

B is correct

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/firewall-placement-for-dos-protection>

upvoted 3 times

[-] 👤 **DavidBackham2020** 2 years, 8 months ago

Selected Answer: B

It is definitely a "Yes" answer.

I would go with B, since you cannot "tailor" the zone protection profile as described in D. You cannot define any device types and OSs in a zone protection profile. <https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-web-interface-help/network/network-network-profiles/network-network-profiles-zone-protection/building-blocks-of-zone-protection-profiles.html#id463e1210-c858-4712-8d34-66b5fb587c2e>

upvoted 3 times

[-] 👤 **homersimpson** 2 years, 8 months ago

Selected Answer: D

Terrible question, it doesn't explain what they mean by "closer". Anyway, if this question is about Zone Protection, then D is correct because the "closer" the fw is to the resources, the more specific the zone protection profile can be. In other words, instead of zone "DMZ" protecting 2 web servers and a file server with a general ZP profile, you can have zone "WEB" with the 2 webservers and zone "FILE" with the file server. Then each zone will have its own specific ZP profile. (Remember that ZP profiles have no specific targets, they only protect a zone in its entirety.

upvoted 3 times

DRAG DROP -

Match each GlobalProtect component to the purpose of that component.

Select and Place:

Answer Area

GlobalProtect Gateway	●		management functions for GlobalProtect infrastructure
GlobalProtect clientless	●		security enforcement for traffic from GlobalProtect apps
GlobalProtect Portal	●		software on endpoints that enables access to network resources
GlobalProtect app	●		secure remote access to common enterprise web applications

Correct Answer:

Answer Area

	●	GlobalProtect Portal	management functions for GlobalProtect infrastructure
	●	GlobalProtect Gateway	security enforcement for traffic from GlobalProtect apps
	●	GlobalProtect app	software on endpoints that enables access to network resources
	●	GlobalProtect clientless	secure remote access to common enterprise web applications

Reference:

<https://docs.paloaltonetworks.com/globalprotect/8-1/globalprotect-admin/globalprotect-overview/about-the-globalprotect-components.html>

Frightened_Acrobat 1 year, 5 months ago

GlobalProtect Clientless VPN provides secure remote access to common enterprise web applications.
<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-clientless-vpn>
 upvoted 1 times

TAKUM1y 1 year, 10 months ago

<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-overview/about-the-globalprotect-components>
 upvoted 1 times

  **kabobmyopic0h** 2 years, 3 months ago

<https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-overview/about-the-globalprotect-components>
upvoted 1 times

  **Shenanigans123** 2 years, 5 months ago



Correct order is:
portal
gateway
app
clientless

As per: <https://docs.paloaltonetworks.com/globalprotect/8-1/globalprotect-admin/globalprotect-overview/about-the-globalprotect-components.html>

and: <https://docs.paloaltonetworks.com/globalprotect/8-1/globalprotect-admin/globalprotect-clientless-vpn.html>
upvoted 4 times

  **Pretorian** 2 years ago

So the order already provided in the answer.
upvoted 5 times

  **sujss** 1 year, 7 months ago

Yeah, why make it complex for the readers. Just say the answer is correct and share the link :)
upvoted 3 times

An administrator needs to validate that policies that will be deployed will match the appropriate rules in the device-group hierarchy. Which tool can the administrator use to review the policy creation logic and verify that unwanted traffic is not allowed?

- A. Preview Changes
- B. Policy Optimizer
- C. Managed Devices Health
- D. Test Policy Match

Correct Answer: D

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/test-policy-rule-traffic-matches.html>

  **datz** Highly Voted 2 years, 3 months ago

Selected Answer: A

Common guys?



"Which tool can the administrator use to review the policy creation logic and verify that unwanted traffic is not allowed?"

which tool is used to review policy creation and also can verify that Unwanted traffic is not allowed?

how on earth Test Policy will tell you what unwanted traffic will be allowed? :/

I am going for A :)


upvoted 5 times

  **Kris92** 9 months, 4 weeks ago

"validate that policies that will be deployed" - preview change

"Which tool can the administrator use to review the policy creation logic and verify that unwanted traffic is not allowed?" - test policy match


upvoted 7 times

  **Kris92** 9 months, 4 weeks ago

pretty simple, you test policy with unwanted traffic and make sure it's denied

how on earth is preview change going to help with that?

upvoted 4 times

  **hcir** Most Recent 2 months ago

Selected Answer: D

You test before adding the rule. Preview Changes only compares the candidate config with the running.

upvoted 1 times

  **Shastings1** 4 months, 2 weeks ago

This is a poorly worded question, but the answer is D - test policy match. Goal here to use a tool to verify that you already have a "deny" rule. Test policy match check the current config for the unwanted traffic. There should be a deny or you need to add another rule. Test policy match source (bad guy) destination (Crown Jewels) action = deny.....

upvoted 1 times

  **VenomX51** 4 months, 4 weeks ago


Selected Answer: A

An administrator needs to validate that policies that will be deployed will match the appropriate rules in the device-group hierarchy.

If you add a policy to device groups for firewall 2 and 3, you can use Preview changes to ensure that that policy is not going to be applied to FW1 and allow unwanted traffic.

Preview Changes will verify your "policy creation logic" - i.e. If I create a policy in this device group it will not be applied to these firewalls.

upvoted 1 times

  **Thunnu** 5 months, 2 weeks ago

Answer D

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/test-policy-rule-traffic-matches>

upvoted 1 times

  **SH_** 7 months ago

Selected Answer: A

"policies that will be deployed" means candidate configuration. and test policy match works on running configuration. so I'm going with A, which I think should be the "preview rule" feature which is on Panorama.

upvoted 1 times

- SH_** 7 months ago
"policies that will be deployed" means candidate configuration. and test policy match works on running configuration. so I'm going with A, which I think should be the "preview rule" feature which is on Panorama.
upvoted 1 times
- JRKhan** 7 months, 3 weeks ago
Selected Answer: A
A is correct. Question is about policies that havent been deployed yet. Test policy match the policies that have already been deployed.
upvoted 1 times
- Metgatz** 7 months, 3 weeks ago
Selected Answer: D
Say check the logic Option D
upvoted 3 times
- Adilon** 8 months ago
D for me
upvoted 2 times
- Whizdhum** 8 months, 3 weeks ago
Selected Answer: A
Answer is A. Preview Changes asks the firewall to compare the configurations you selected in the Commit Scope to the running configuration. The answer is not Test Policy Match, which tests policy rules in your running configuration. Preview Changes is pre-commit, Test Policy Match is post-commit.
upvoted 2 times
- dorf05** 8 months, 4 weeks ago
Selected Answer: D
preview (before) commit and review (after commit). and the question is "administrator use to review the policy creation and verify that unwanted traffic is not allowed". this similar to question # 1
upvoted 2 times
- Metgatz** 8 months, 4 weeks ago
The correct option is D Test Policy Match
upvoted 2 times
- scanossa** 9 months, 2 weeks ago
Selected Answer: D
The question doesn't say "preview", it says "review". It could involve rules already deployed, som answer D.
Answer A doesn't show if a specific traffic is allowed or not
upvoted 1 times
- RoamingFo** 9 months, 2 weeks ago
Selected Answer: D
Preview will only show the changes, which is not enough to determine if traffic will be allowed or denied. This is a collective result of all the rules old and new.
I think D is the most acceptable answer for this poorly worded question.
upvoted 1 times
- Omid2022** 10 months, 1 week ago
Selected Answer: A
Test policy match works after committing the config, so you belowed up the network then you want to check it!!!
upvoted 1 times
- dgonz** 1 year ago
Selected Answer: D
it asks for "which tool"
not sure if the preview pane can be considered as a tool...
so I choose D, which is a tool
upvoted 1 times

What is a key step in implementing WildFire best practices?

- A. Configure the firewall to retrieve content updates every minute.
- B. Ensure that a Threat Prevention subscription is active.
- C. In a mission-critical network, increase the WildFire size limits to the maximum value.
- D. In a security-first network, set the WildFire size limits to the minimum value.

Correct Answer: B

Reference:



<https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-deployment-best-practices/wildfire-best-practices>

  **bartbernini** Highly Voted 2 years, 6 months ago

Selected Answer: B

B is correct. In the WildFire best practices linked below, the first step is to "... make sure that you have an active Threat Prevention subscription. Together, WildFire® and Threat Prevention enable comprehensive threat detection and prevention."

<https://docs.paloaltonetworks.com/wildfire/10-1/wildfire-admin/wildfire-deployment-best-practices/wildfire-best-practices.html>
upvoted 8 times

  **Marcy** Highly Voted 2 years, 8 months ago

B is correct.
upvoted 5 times

  **TAKUM1y** Most Recent 1 year, 10 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/wildfire-deployment-best-practices/wildfire-best-practices>
upvoted 2 times

What happens when an A/P firewall cluster synchronizes IPsec tunnel security associations (SAs)?

- A. Phase 2 SAs are synchronized over HA2 links.
- B. Phase 1 and Phase 2 SAs are synchronized over HA2 links.
- C. Phase 1 SAs are synchronized over HA1 links.
- D. Phase 1 and Phase 2 SAs are synchronized over HA3 links.

Correct Answer: B

bartbernini Highly Voted 2 years, 6 months ago

Selected Answer: A

From the Palo Alto documentation below, "when a VPN is terminated on a Palo Alto firewall HA pair, not all IPSEC related information is synchronized between the firewalls... This is an expected behavior. IKE phase 1 SA information is NOT synchronized between the HA firewalls."

And from the second link, "Data link (HA2) is used to sync sessions, forwarding tables, IPsec security associations, and ARP tables between firewalls in the HA pair. Data flow on the HA2 link is always unidirectional (except for the HA2 keep-alive). It flows from the active firewall to the passive firewall."

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW&lang=en_US%E2%80%A9&refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail

<https://help.aryaka.com/display/public/KNOW/Palo+Alto+Networks+NFV+Technical+Brief>

upvoted 18 times

Marcy Highly Voted 2 years, 8 months ago

Correct. Only Phase2 are Synced.

upvoted 7 times

Metgatz Most Recent 8 months, 4 weeks ago

Correct option is A : This is an expected behavior. IKE phase 1 SA information is NOT synchronized between the HA firewalls -

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW>

upvoted 1 times

gc999 10 months, 1 week ago

Selected Answer: A

I believe A is the answer

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIXGCA0#:~:text=Session%20states-,IPsec%20SAs,-MAC%20Tables>

upvoted 1 times

Omid2022 10 months, 1 week ago

Selected Answer: A

Study guide page 194:

The HA2 link is used to synchronize sessions, forwarding tables, IPsec security associations and ARP tables between firewalls in an HA pair. Data flow on the HA2 link is always unidirectional (except for the HA2 keep-alive); it flows from the active or active-primary firewall to the passive or active-secondary firewall. The HA2 link is a Layer 2 link, and it uses ether type 0x7261 by default

upvoted 1 times

jhonelo2011 11 months, 3 weeks ago

Selected Answer: B

I am going with B, Phase 1 and 2 are part of IPsec VPN tunnels.

upvoted 1 times

TAKUM1y 1 year, 10 months ago

Selected Answer: B



<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/ha-links-and-backup-links#id1df2d565-1765-4666-83b0-87652318e06f>

upvoted 2 times

yup101 1 year, 9 months ago

It's A. bertbernini URL explains it pretty well.

upvoted 2 times

  **ericli87** 1 year, 4 months ago
Phase1 is IKE SA. Phase 2 is IPSEC SA.
upvoted 1 times

Question #257

Topic 1




A security engineer needs to mitigate packet floods that occur on a set of servers behind the internet facing interface of the firewall.
Which Security Profile should be applied to a policy to prevent these packet floods?





- A. Vulnerability Protection profile
- B. DoS Protection profile
- C. Data Filtering profile
- D. URL Filtering profile



Correct Answer: B



Reference:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles>

  **Marcy**  2 years, 8 months ago
B is correct.
upvoted 9 times

  **Sammy3637**  8 months, 3 weeks ago

B no doubt !
upvoted 1 times

  **Pretorian** 2 years ago
DoS Protection Profile should be applied to a DoS policy
upvoted 2 times

  **shinichi_88** 2 years, 7 months ago
B, 100%
upvoted 4 times

What are three reasons why an installed session can be identified with the "application incomplete" tag? (Choose three.)

- A. There was no application data after the TCP connection was established.
- B. The client sent a TCP segment with the PUSH flag set.
- C. The TCP connection was terminated without identifying any application data.
- D. There is not enough application data after the TCP connection was established.
- E. The TCP connection did not fully establish.

Correct Answer: ADE

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC>

  **imokenzo** Highly Voted 2 years, 8 months ago

ACE is my thought.

D is eliminated due to falling into "insufficient data"

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC>



upvoted 15 times

  **Metgatz** Most Recent 7 months, 3 weeks ago

Selected Answer: ACE

A,C,E are the best options

upvoted 1 times



  **Metgatz** 8 months, 4 weeks ago

Incomplete in the application field:

Incomplete means that either the three-way TCP handshake did not complete OR the three-way TCP handshake did complete but there was not enough data after the handshake to identify the application. In other words that traffic being seen is not really an application.

One example is, if a client sends a server a SYN and the Palo Alto Networks device creates a session for that SYN , but the server never sends a SYN ACK back to the client, then that session is incomplete.

upvoted 1 times

  **sujss** 1 year, 4 months ago

Selected Answer: ACE

D = insufficient data

upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

C is most likely a cause of Unknown-tcp, TCP handshake, but the application was not identified. I presumed the correct answer is ADE.



Incomplete means that either the three-way TCP handshake did not complete OR the three-way TCP handshake did complete but there was "NO ENOUGH" data after the handshake to identify the application. In other words that traffic being seen is not really an application.

upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

Reading it again. I'm going for ACE.

upvoted 2 times

  **scally** 1 year, 11 months ago

Selected Answer: ACE

Incomplete means that either the three-way TCP handshake did not complete OR the three-way TCP handshake did complete but there was not enough data after the handshake to identify the application. In other words that traffic being seen is not really an application.

One example is, if a client sends a server a SYN and the Palo Alto Networks device creates a session for that SYN , but the server never sends a SYN ACK back to the client, then that session is incomplete.

Insufficient data means not enough data to identify the application. So for example, if the three-way TCP handshake completed and there was one data packet after the handshake but that one data packet was not enough to match any of our signatures, then user will see insufficient data in the application field of the traffic log.

upvoted 4 times

  **secdaddy** 2 years ago

ADE makes sense - from the KB :

"Incomplete means that either the three-way TCP handshake did not complete (E) OR the three-way TCP handshake did complete but there was no

enough data after the handshake to identify the application." (A and D both)

upvoted 1 times

  **secdaddy** 2 years ago

Never mind - I see your point re D = insufficient data.

upvoted 1 times

  **harrypogi** 2 years, 3 months ago

A is wrong. If TCP connection was established yet App-ID still doesn't have enough data to identify the application. The application must be flag as unknown-tcp or unknown-udp.

upvoted 2 times

  **scanossa** 6 months, 1 week ago

but A doesn't say "not enough", it says "no application data" at all. So it is a different scenery

upvoted 1 times

  **lildevil** 1 year, 2 months ago

I gotta ask...how many TCP connections you see established yet get flagged as unknown-udp ?

upvoted 1 times

  **datz** 2 years, 3 months ago

Selected Answer: ACE

WRONG - D - There is not enough application data after the TCP connection was established. | Not enough APP Data meaning - Insufficient data in the application field:

B - Cant B

So answer: ACE

Incomplete in the application field:

Incomplete means that either the three-way TCP handshake did not complete OR the three-way TCP handshake did complete but there was not enough data after the handshake to identify the application. In other words that traffic being seen is not really an application.

One example is, if a client sends a server a SYN and the Palo Alto Networks device creates a session for that SYN , but the server never sends a SYN ACK back to the client, then that session is incomplete.

Insufficient data in the application field:

Insufficient data means not enough data to identify the application. So for example, if the three-way TCP handshake completed and there was one data packet after the handshake but that one data packet was not enough to match any of our signatures, then user will see insufficient data in the application field of the traffic log.

upvoted 2 times

  **AbuHussain** 2 years, 5 months ago

Selected Answer: ACE

its ACE

upvoted 2 times

  **shinichi_88** 2 years, 7 months ago

ACE, just checked

upvoted 1 times

  **hairysnowman** 2 years, 8 months ago

ACE is my thought as well.

E would come up as 'incomplete' in the logs because the tcp session never fully establishes; i.e., the firewall didn't capture the threeway handshake.

upvoted 3 times

  **hairysnowman** 2 years, 8 months ago

I meant ACD*.

upvoted 1 times

  **hairysnowman** 2 years, 8 months ago

Ugh...just reread the question. ACE is right because of incomplete.

Need more coffee...

upvoted 5 times

  **GivemeMoney** 2 years, 7 months ago

ACE is right!

D falls under Insufficient data and the question is for "application incomplete".

upvoted 2 times

  **Elvenking** 2 years, 4 months ago

E is out because the session was installed per the question text.

upvoted 1 times

 **Loloshikovichev** 2 years, 4 months ago

As per palo document: Incomplete means that either the three-way TCP handshake did not complete
That means - session will be created after initial SYN packet. If no packets were seen and session expired with only 1 SYN app will be incomplete. So E is the correct option.

upvoted 2 times

Which three statements correctly describe Session 380280? (Choose three.)

```
> show session id 380280
Session                               380280
c2s flow:
  source:                             172.17.149.129 [L3-Trust]
  dst:                                 104.154.09.105
  proto:                               6
  sport:                              60997           dport:          443
  state:                              ACTIVE           type:          FLOW
  src user:                            unknown
  dst user:                            unknown

s2c flow:
  source:                             104.154.89.105 [L3-Untrust]
  dst:                                 10.46.42.149
  proto:                               6
  sport:                              443           dport:          7260
  state:                              ACTIVE           type:          FLOW
  src user:                            unknown
  dst user:                            unknown

start time                            : Tue Feb 9 20:38:42 2021
timeout                                : 15 sec
time to live                           : 2 sec
total byte count (c2s)                 : 3330
total byte count (s2c)                 : 12698
layer7 packet count (c2s)              : 14
layer7 packet count (s2c)              : 19
vsys                                    : vsys1
application                            : web-browsing
rule                                    : Trust-to-Untrust
service timeout override (index)       : False
session to be logged at end            : True
session in session ager                 : True
session updated by HA peer             : False
session proxied                        : True
address/port translation                : source
nat-rule                               : Trust-NAT (vsys1)
Layer7 processing                      : Completed
URL filtering enabled                   : True
URL category                           : computer-and-internet-info, low-risk
session via syn-cookies                 : False
session terminated on host              : False
session traverses tunnel                : False
session terminate tunnel                : False
captive portal session                 : False
ingress interface                      : etheriet1/6
egress interface                       : ethernet1/3
session GOS rule                       : N/A (class 4)
tracker stage 17proc                   : proxy timer expired
end-reason                             : unknown
```

- A. The application was initially identified as "ssl."
- B. The session has ended with the end-reason "unknown."
- C. The session did not go through SSL decryption processing.
- D. The application shifted to "web-browsing."
- E. The session went through SSL decryption processing.

Correct Answer: BDE

[-] 👤 **Shenanigans123** Highly Voted 2 years, 5 months ago

There is a lack of available documentation for this CLI command.

I think the answer is ADE

Cannot be B because session is still active, hence reason "unknown"

I don't think it can be C because "session proxied" is true which I've only seen when SSL Decryption is being performed - regular HTTP traffic does not show this flag

upvoted 10 times

[-] 👤 **Loloshikovichev** 2 years, 4 months ago

I agree, ADE seems to be correct.

upvoted 3 times

[-] 👤 **Loloshikovichev** Highly Voted 2 years, 4 months ago

Selected Answer: ADE

ADE is correct. Session is still active, hence 'unknown' end reason, as mentioned correctly by Shenanigans123.

upvoted 6 times

[-] 👤 **Bau24** Most Recent 1 month, 3 weeks ago

Selected Answer: ADE

Correct answers: ADE

upvoted 1 times

[-] 👤 **ansibai** 8 months, 1 week ago

Selected Answer: ADE

I perform this in lab.

upvoted 1 times

[-] 👤 **Whizdhum** 8 months, 3 weeks ago

Answers are A, D, E.

upvoted 1 times

[-] 👤 **seb_berlin** 8 months, 3 weeks ago

Selected Answer: ADE

Got his question in December 2023

only good two choices to answer.

selected D and E

as others already stated end-reason "unkown" is misleading look at the state = ACTIVE

session table = actual sessions

upvoted 1 times

[-] 👤 **Metgatz** 8 months, 4 weeks ago

ADE is the correct option

upvoted 1 times

[-] 👤 **network_020** 9 months, 2 weeks ago

Session Proxied : Yes means session is ssl decrypted

Before decryption identified as ssl and after decryption identified as web browsing

upvoted 3 times

[-] 👤 **procheeseburger** 1 year, 2 months ago

when I had this question, it only asked for 2 things.

upvoted 1 times

[-] 👤 **PANW** 1 year, 6 months ago

How do you know from this info that the session was decrypted?

You can infer it from the question by a process of elimination, B&C are wrong

upvoted 1 times

[-] 👤 **sujss** 1 year, 4 months ago

I believe from "Session Proxied : Yes"

upvoted 2 times

[-] 👤 **wallaka** 9 months, 1 week ago


Port 443 and app web-browsing is a clue as well.

upvoted 1 times


[-] 👤 **PANW** 1 year, 6 months ago

the sh session command only shows active sessions, can't be B

upvoted 1 times

[-]  **DenskyDen** 1 year, 7 months ago


ADE. The fact that the session is still active, it can't be B.
upvoted 1 times

[-]  **Sarbi** 1 year, 8 months ago

ADE is correct. As the initial traffic is on port 443 and after that application shift occurs and the session is still active.
upvoted 1 times

[-]  **mz101** 1 year, 9 months ago

Should be ADE.
"end reason: unknown" will show for all "ACTIVE" sessions. So B is not correct.
upvoted 1 times

[-]  **scally** 1 year, 11 months ago

Selected Answer: BDE

With the destination port being 443 and the application being web-browsing, that means that this was decrypted. The session clearly says it ended as unknown.
upvoted 3 times

[-]  **Knowledge33** 1 year, 3 months ago

on session id, we always have the end reason field fulfilled. "unknown means there is nothing. In other word, the session is still active. When the session is ended, you have different things such as INIT or other
upvoted 2 times

[-]  **tenebrox** 2 years, 2 months ago

Selected Answer: BDE

end session unknow is a valid en reason
upvoted 1 times

[-]  **TMoose** 2 years, 3 months ago

unknown—This value applies in the following situations:
Session terminations that the preceding reasons do not cover (for example, a clear session all command).
For logs generated in a PAN-OS release that does not support the session end reason field (releases older than PAN-OS 6.1), the value will be unknown after an upgrade to the current PAN-OS release or after the logs are loaded onto the firewall.
In Panorama, logs received from firewalls for which the PAN-OS version does not support session end reasons will have a value of unknown. BDE
upvoted 1 times

[-]  **Gngogh** 1 year, 10 months ago

The fact is that the session is still in the ACTIVE state, therefore the answer "the session has ended with the end-reason unknown" is not valid, because the session hasn't ended.
upvoted 1 times

[-]  **Gngogh** 1 year, 10 months ago

When the session ends the state changes to INIT.
upvoted 1 times

An administrator's device-group commit push is failing due to a new URL category.
How should the administrator correct this issue?

- A. update the Firewall Apps and Threat version to match the version of Panorama
- B. change the new category action to "alert" and push the configuration again
- C. ensure that the firewall can communicate with the URL cloud
- D. verify that the URL seed tile has been downloaded and activated on the firewall

Correct Answer: A

  **Mucho9999** Highly Voted  2 years, 8 months ago

Selected Answer: A

The answer is A not C

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNqw>

upvoted 12 times

  **GivemeMoney** 2 years, 7 months ago

Thanks for the link! - Unable to perform commit to Firewall from the Panorama due to new URL Filtering Categories.

upvoted 1 times

  **Marcy** Highly Voted  2 years, 8 months ago

I think its A.. from experience.

A. update the Firewall Apps and Threat version to match the version of Panorama

upvoted 7 times

  **Sammy3637** Most Recent  8 months, 3 weeks ago

Selected Answer: A

A - App and threat version should match between Panorama and the managed firewall

upvoted 1 times

  **Khs01** 2 years ago

Selected Answer: A

Correct, is A

upvoted 2 times

  **GivemeMoney** 2 years, 7 months ago

Selected Answer: A

Mucho9999 is right. A. update the Firewall Apps and Threat version to match the version of Panorama

upvoted 3 times



A security engineer needs firewall management access on a trusted interface. Which three settings are required on an SSL/TLS Service Profile to provide secure Web UI authentication? (Choose three.)

- A. Authentication Algorithm
- B. Encryption Algorithm
- C. Certificate
- D. Maximum TLS version
- E. Minimum TLS version



Correct Answer: CDE

Reference:



<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/certificate-management/configure-an-ssl-tls-service-profile>

  **Metgatz** 8 months, 4 weeks ago

- C. Certificate
 - D. Maximum TLS version
 - E. Minimum TLS version
- upvoted 2 times

  **sov4** 1 year, 1 month ago

On the exam, July 2023
upvoted 3 times

  **sov4** 1 year, 1 month ago

CDE btw
upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago



Selected Answer: CDE

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/configure-an-ssl-tls-service-profile>
upvoted 4 times

  **UFanat** 2 years, 2 months ago

Selected Answer: CDE

CDE
checked i a lab
upvoted 4 times

  **NLT** 2 years, 6 months ago

Select DeviceCertificate ManagementSSL/TLS Service Profile.
If the firewall has more than one virtual system (vsys), select the Location (vsys or Shared) where the profile is available.
Click Add and enter a Name to identify the profile.
Select the Certificate you just obtained.
Define the range of protocols that the service can use:
For the Min Version, select the earliest allowed TLS version: TLSv1.0 (default), TLSv1.1, or TLSv1.2.
For the Max Version, select the latest allowed TLS version: TLSv1.0, TLSv1.1, TLSv1.2, or Max (latest available version). The default is Max.
upvoted 2 times



Which type of interface does a firewall use to forward decrypted traffic to a security chain for inspection?

- A. Layer 3
- B. Layer 2
- C. Tap
- D. Decryption Mirror

Correct Answer: A



Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/decryption-broker/decryption-broker-concepts/decryption-broker-forwarding-interfaces.html#:~:text=A%20firewall%20enabled%20as%20a%20security%20chain%20for%20inspection>

  **Sammy3637** 8 months, 3 weeks ago

Selected Answer: A

It asks which 'interface' , Decryption mirror is not an interface
upvoted 1 times

  **BT22** 1 year, 2 months ago

Ans is D
upvoted 3 times

  **mz101** 1 year, 9 months ago

Should be A.
Decryption Mirror should mainly for DLP kind of devices, without coming "back" traffic.
upvoted 1 times



  **TAKUM1y** 1 year, 10 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/decryption-broker/decryption-broker-concepts/decryption-broker-security-chain-layer-3#id182QM0B0S9D>
upvoted 3 times

  **mysteryzjoker** 1 year, 10 months ago

it is a nasty question. I guess it receives on the decryption mirror and forwards out layer 3.
upvoted 3 times



  **UFanat** 2 years, 2 months ago

Selected Answer: A



Decryption Broker: Forwarding Interfaces
A firewall enabled as a decryption broker uses a pair of dedicated Layer 3 interfaces to forward decrypted traffic to a security chain for inspection. The decryption forwarding interfaces must be assigned to a brand new virtual router
<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/decryption-broker/decryption-broker-concepts/decryption-broker-forwarding-interfaces>
upvoted 2 times

  **poiuytr** 2 years, 4 months ago

Answer: A - layer 3
"A firewall enabled as a decryption broker uses a pair of dedicated Layer 3 interfaces to forward decrypted traffic to a security chain for inspection."
<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/decryption-broker/decryption-broker-concepts/decryption-broker-forwarding-interfaces>
upvoted 1 times

  **NLT** 2 years, 6 months ago

Follow these guidelines to set up Layer 3 security chain devices to support decryption broker:
Configure security chain devices with Layer 3 interfaces to connect to the security chain network. These Layer 3 interfaces must have an assigned IP address and subnet mask.
upvoted 1 times

  **DavidBackham2020** 2 years, 7 months ago

This is a shitty question. Assuiming, the firewall is decrypting the traffic, I would go with D:
<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/decryption-concepts/decryption-mirroring.html>
Assuming the firewall is part of a Security Chain and the traffic is already decrypted (not decrypted on the firewall), I would go with A:
<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/network-packet-broker/configure-routed-layer-3-security-chains>
upvoted 2 times

  **drrealest** 2 years, 8 months ago

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/network-packet-broker/configure-routed-layer-3-security-chains>
upvoted 1 times

  **Marcy** 2 years, 8 months ago

Initially thought it was D but A is correct.

Configure security chain devices with Layer 3 interfaces to connect to the security chain network. These Layer 3 interfaces must have an assigned IP address and subnet mask.

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/decryption-broker/security-chain-layer-3-guidelines.html>
upvoted 4 times

An administrator cannot see any Traffic logs from the Palo Alto Networks NGFW in Panorama reports. The configuration problem seems to be on the firewall.

Which settings, if configured incorrectly, most likely would stop only Traffic logs from being sent from the NGFW to Panorama?

A.

Security Policy Rule ?

General | Source | Destination | Application | Service/URL Category | Actions | Usage

Action Setting

Actions: Allow ▼

Send ICMP unreachable

Log Setting

Log at Session Start

Log at Session End

Log Forwarding: None ▼

Profile Setting

Profile Type: Profiles ▼

Antivirus: default ▼

Vulnerability Protections: strict ▼

Anti-Spyware: strict ▼

URL Filtering: default ▼

File Blocking: None ▼

Data Filtering: None ▼

WildFire Analysis: default ▼

Other Settings

Schedule: None ▼

QoS Marking: None ▼

Disable Server Responsive Inspection

OK
Cancel

B.

Syslog Server Profile ?

Name: SyslogProfile1

Servers | Custom Log Format

NAME	SYSLOG SERVER	TRANSPORT	PORT	FORMAT	FACILITY
SyslogServer1	192.168.229.17	UDP	514	BSD	LOG_USER

+ Add - Delete

Enter the IP address or FQDN of the Syslog server

OK
Cancel

C.

Panorama Settings



Receive Timeout for Connection to Device (sec) 240

Send Timeout for Connection to Device (sec) 240

Retry Count for SSL Send to Device 25

Share Unused Address and Service Objects with Devices

Objects defined in ancestors will take higher precedence

Enable reporting and filtering on groups

When enabled Panorama will locally store users and groups from Master Devices

OK

Cancel

D.

Panorama Settings

Panorama Servers

10.99.1.21

Enable pushing device monitoring data to Panorama

Receive Timeout for Connection to Panorama (sec) 240

Send Timeout for Connection to Panorama (sec) 240

Retry Count for SSL Send to Panorama 25

Enable automated commit recovery

Number of attempts to check for Panorama connectivity 1

Interval between retries (sec) 10

Disable Panorama Policy and Objects

Disable Device and Network Template

OK

Cancel

Correct Answer: A

Marcy Highly Voted 2 years, 8 months ago

It is A.

upvoted 9 times

Plato22 Highly Voted 2 years, 8 months ago

Correct answer is A.

upvoted 6 times

Metgatz Most Recent 8 months, 4 weeks ago

A Missing Log forwarding profile

upvoted 1 times

  **AbuHussain** 2 years, 5 months ago

A is correct

upvoted 2 times

  **Mp84047** 2 years, 5 months ago

A is correct So the question here is different than it was originally. It clearer now, if that's possible in a PCNSE test. but it says stop logging if configured incorrectly so only A

upvoted 3 times

  **GivemeMoney** 2 years, 7 months ago

Hey admin, correct answer is: A! Log forwarding should be set!

upvoted 4 times

  **hairysnowman** 2 years, 8 months ago

A.

No log forwarding profile has been selected to the send the logs.

upvoted 4 times

  **Gogosa** 2 years, 8 months ago

A is correct

upvoted 3 times

Which configuration task is best for reducing load on the management plane?

- A. Enable session logging at start
- B. Disable logging on the default deny rule
- C. Set the URL filtering action to send alerts
- D. Disable pre-defined reports

Correct Answer: D

  **Sammy3637** 8 months, 3 weeks ago

Selected Answer: D

Disable predefined reports
upvoted 1 times

  **awtsuriticuna** 1 year, 9 months ago

Option D

Report generation can also consume considerable resources, while some pre-defined reports may not be useful to the organization, or they've been replaced by a custom report. These pre-defined reports can be disabled from Device > Setup > Logging and Reporting Settings

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CISvCAK>

upvoted 1 times



  **confusion** 1 year, 10 months ago

Selected Answer: D

B is enabled by default, so we can exclude it --> D is the correct answer.
upvoted 2 times


  **homersimpson** 8 months, 2 weeks ago

Logging is NOT enabled on the default deny rule.
upvoted 1 times

  **bimyo** 1 year, 11 months ago

Can you help my thought process out here as both B (Disable logging on the default deny rule) and D (Disable pre-defined reports) will reduce the CP load. What am I missing, as D seems to be the correct answer, but based on what can I discard B? Thanks!

upvoted 1 times

  **secdaddy** 1 year, 11 months ago

By default logging is disabled on the default deny rule
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIHkCAK>
Pre-defined reports are (maybe - I don't have a way to test) enabled by default :
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CISvCAK>
upvoted 1 times

An engineer is in the planning stages of deploying User-ID in a diverse directory services environment. Which server OS platforms can be used for server monitoring with User-ID?

- A. Microsoft Active Directory, Red Hat Linux, and Microsoft Exchange
- B. Microsoft Terminal Server, Red Hat Linux, and Microsoft Active Directory
- C. Novell eDirectory, Microsoft Terminal Server, and Microsoft Active Directory
- D. Microsoft Exchange, Microsoft Active Directory, and Novell eDirectory

Correct Answer: B

Reference:

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/user-id-concepts/user-mapping/server-monitoring.html>



  **ali_sh85** 1 month, 2 weeks ago

Selected Answer: D

correct answer should be D

Microsoft Terminal Server is used for terminal services, and while it can be involved in User-ID, it is not a primary directory service. Red Hat Linux is not typically used for User-ID server monitoring.

upvoted 1 times

  **Od2fdfa** 3 months, 2 weeks ago

Why it says correct answer is B

It is incorrect.

Correct answer is D as per documentation.



upvoted 1 times

  **b8c290d** 4 months, 1 week ago

D

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/user-id-concepts/user-mapping/server-monitoring#:~:text=With%20server%20monitoring%20a%20User,eDirectory%20servers%20for%20login%20events.>

upvoted 1 times

  **Metgatz** 8 months, 4 weeks ago

D is the correct option



upvoted 2 times

  **Vahid4900** 1 year, 5 months ago

Selected Answer: D

Answer is D. Four choices listed in config: MS AD, MS Exchange, Novell eDir, and Syslog Sender.

upvoted 4 times

  **Sarbi** 1 year, 8 months ago

100 d.With server monitoring a User-ID agent—either a Windows-based agent running on a domain server in your network, or the PAN-OS integrated User-ID agent running on the firewall—monitors the security event logs for specified Microsoft Exchange Servers, Domain Controllers, or Novell eDirectory servers for login events.

upvoted 2 times

  **djedeen** 1 year, 9 months ago

Selected Answer: D

Answer is D. Four choices listed in config: MS AD, MS Exchange, Novell eDir, and Syslog Sender.

upvoted 1 times

  **confusion** 1 year, 10 months ago

Selected Answer: D

D shall be correct.

upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/user-id-concepts/user-mapping/server-monitoring>

upvoted 3 times

  **Alen** 1 year, 11 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/user-id/user-id-concepts/user-mapping/server-monitoring>
upvoted 1 times

  **mizuno92** 1 year, 11 months ago



Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/user-id-concepts/user-mapping/server-monitoring>
upvoted 1 times

  **mushi4ka** 1 year, 11 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/user-id-concepts/user-mapping/server-monitoring>
upvoted 1 times

  **nose999** 2 years ago

Selected Answer: D

<https://docs.paloaltonetworks.com/compatibility-matrix/user-id-agent/which-servers-can-the-user-id-agent-monitor>
upvoted 2 times

Cortex XDR notifies an administrator about grayware on the endpoints. There are no entries about grayware in any of the logs of the corresponding firewall. Which setting can the administrator configure on the firewall to log grayware verdicts?

- A. in Threat General Settings, select "Report Grayware Files"
- B. within the log settings option in the Device tab
- C. in WildFire General Settings, select "Report Grayware Files"
- D. within the log forwarding profile attached to the Security policy rule

Correct Answer: D

  **nose999** Highly Voted  2 years ago

Selected Answer: C



<https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/monitor-wildfire-activity/use-the-firewall-to-monitor-malware/configure-wildfire-submissions-log-settings/enable-logging-for-benign-and-grayware-samples>

upvoted 8 times

  **123XYZT** Most Recent  3 months ago



D
Log Forwarding Profile Match List
Log Type: wildfire
Filter verdict eq grayware

upvoted 2 times

  **1f2c588** 3 months, 3 weeks ago

answer is C: configure report grayware files on the device, setup, wildfire, general settings



upvoted 1 times

  **Whizdhum** 8 months, 3 weeks ago

Selected Answer: C

Answer is C. When this option is enabled (disabled by default), files analyzed by WildFire that are determined to be grayware will appear in the Monitor > WildFire Submissions log.



upvoted 2 times

  **Sammy3637** 8 months, 3 weeks ago

Selected Answer: C

Under Wildfire settings --> Report Grayware

upvoted 1 times

  **Sarbi** 1 year, 8 months ago

Looks c is more accurate. As first we have to select report grayware . The only it will logs

upvoted 2 times

  **confusion** 1 year, 10 months ago

Selected Answer: C

Definitely C, otherwise they won't be logged.

upvoted 3 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/wildfire/10-2/wildfire-admin/monitor-wildfire-activity/use-the-firewall-to-monitor-malware/configure-wildfire-submissions-log-settings/enable-logging-for-benign-and-grayware-samples>

upvoted 3 times

  **Kuronekosama** 1 year, 10 months ago

Selected Answer: D

C turn on verdicts. D turns on the logging.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CITqCAK>

upvoted 2 times

  **Kuronekosama** 1 year, 10 months ago



Nevermind. Answer is C.

It turns on logging to wildfire submissions upon report Gray ware Files.

Your company has 10 Active Directory domain controllers spread across multiple WAN links. All users authenticate to Active Directory. Each link has substantial network bandwidth to support all mission-critical applications. The firewall's management plane is highly utilized. Given this scenario, which type of User-ID agent is considered a best practice by Palo Alto Networks?

- A. PAN-OS integrated agent
- B. Citrix terminal server agent with adequate data-plane resources
- C. Captive Portal
- D. Windows-based User-ID agent on a standalone server



Correct Answer: D

  **avator** 7 months, 2 weeks ago

Selected Answer: D
Which Agent Type is Better?

The result is that, in an infrastructure with remote networks separated by WAN links, the integrated agent is more appropriate for reading remote logs and the Windows-based agent is more appropriate for reading local logs. However, use of the integrated agent is not without cost: It consumes more of the firewall's management plane resources. For this reason, deployment of the Windows agent at remote sites and having them forward the relevant User-ID information to a firewall on a central network often is beneficial.

https://beacon.paloaltonetworks.com/uploads/resource_courses
upvoted 1 times

  **Whizdhum** 8 months, 3 weeks ago

Answer is D. The way you configure the User-ID agent depends on the size of your environment and the location of your domain servers. As a best practice, locate your User-ID agents near the servers it will monitor (that is, the monitored servers and the Windows User-ID agent should not be across a WAN link from each other).

upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

D. Read TAKUM1y link.
upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-mapping-using-the-windows-user-id-agent>
upvoted 3 times

Which component enables you to configure firewall resource protection settings?

- A. DoS Protection Profile
- B. QoS Profile
- C. Zone Protection Profile
- D. DoS Protection policy

Correct Answer: D

[-] **Sarbi** Highly Voted 1 year, 8 months ago

The question is firewall resource protection not end device resource protection. So I think it is C is correct.
upvoted 17 times

[-] **Moadil_001** Most Recent 1 day, 2 hours ago

Selected Answer: C

Its "C"

Resource protection settings are generally related to protecting the firewall itself from being overwhelmed by excessive or malicious traffic, which is why they are configured within a Zone Protection Profile. This profile ensures that the firewall's resources are not exhausted by attacks at the network level.

A DoS Protection Profile, on the other hand, is more targeted and is used to protect specific internal resources from being overwhelmed by traffic directed at them.

upvoted 1 times

[-] **ali_sh85** 1 month, 2 weeks ago

Selected Answer: A

Answer is A we can define the Resources Protection under Dos Protection Profile

upvoted 1 times

[-] **jeremykebir** 1 month, 3 weeks ago

Guy's 100% it's C

It's about firewall resource protection and not end device.

End Device is related to DoS Protection profile

upvoted 1 times

[-] **SkyderAmzLee** 1 month, 3 weeks ago

Selected Answer: C

same with VenomX51

upvoted 1 times

[-] **VenomX51** 5 months ago

Selected Answer: C

As already stated:

Zone Protection Profile protects the firewall's resources.

DoS Protection Profile protects the client/server's resources.

upvoted 1 times

[-] **netsof** 6 months, 1 week ago

Selected Answer: C

DoS protection protects individual critical servers/devices, the question asks for Firewall resources so it should be Zone protection profile.

upvoted 2 times

[-] **Merlin0o** 6 months, 4 weeks ago

Selected Answer: C

Answer should be C

As taken from p48m1 "

Zone Protection Profile protects the firewall's resources.

DoS Protection Profile protects the client/server's resources."

upvoted 1 times

[-] **Whizdhum** 8 months, 3 weeks ago

Selected Answer: A

Answer is A. You specify a DoS protection profile in a DoS protection policy rule, where you specify the criteria for packets to match the rule, and the policy rule determines the devices to which the profile applies. Resource Protection Profile limits the maximum number of concurrent sessions.

upvoted 2 times

mfreeman45770 8 months, 3 weeks ago

DoS Protection profiles set thresholds that protect against new session IP flood attacks and provide resource protection (maximum concurrent session limits for specified endpoints and resources).

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules/dos-protection-profiles>

upvoted 1 times

mfreeman45770 8 months, 3 weeks ago

DOS is for specific endpoints, Zone is for the firewall itself so it all depends on how you think they intended the question be interpreted

upvoted 1 times

Sammy3637 8 months, 3 weeks ago

Selected Answer: C

C looks correct like other mentioned keyword 'FW Resource protection "

upvoted 1 times

Metgatz 8 months, 4 weeks ago

Resource protection is part of "DoS Protection Profile" the correct answer is A - <https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules/dos-protection-profiles#ida42d52fa-3366-4695-bb4a-d39ebf3b6a5f~:text=aggregate%20profiles%2C%20the-,Resources%20Protection,-threshold%20applies%20to>

upvoted 2 times

Omid2022 9 months, 1 week ago

Selected Answer: C

In the context of the following paloalto website article, the component that enables you to configure firewall resource protection settings is Zone Protection. Zone Protection is specifically mentioned as a measure to defend against Slow Path DoS Attacks on the firewall's resources. It tracks the connection-per-second rate incoming to a Zone, aggregating all connection-per-second rates for each protocol coming in on all interfaces tied to the protected Zone:

SLOW PATH DOS ATTACKS AGAINST THE FIREWALL

To defend the firewall resources from a Slow Path DoS Attack, use Zone Protection - Flood Protection.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000sY1pCAE>

upvoted 1 times

Xuzi 9 months, 3 weeks ago

Selected Answer: A

DoS Protection Profiles

DoS Protection profiles provide detailed control for Denial of Service (DoS) protection policy rules. DoS policy rules allow you to control the number of sessions between interfaces, zones, addresses, and countries based on aggregate sessions or source and/or destination IP addresses. There are two DoS protection mechanisms that the Palo Alto Networks firewalls support.

Flood Protection—Detects and prevents attacks where the network is flooded with packets resulting in too many half-open sessions and/or services being unable to respond to each request. In this case, the source address of the attack is usually spoofed. See DoS Protection Against Flooding of New Sessions.

Resource Protection— Detects and prevent session exhaustion attacks. In this type of attack, a large number of hosts (bots) are used to establish as many fully established sessions as possible to consume all of a system's resources.

upvoted 1 times

Omid2022 10 months, 1 week ago

Selected Answer: C

I go for C since you can enable it globally on the firewall and a zone protection profile is a component that enables you to configure firewall resource protection settings for a zone. A zone protection profile allows you to set thresholds for various types of attacks, such as SYN floods, ICMP floods, UDP floods, and IP fragments. A DoS Protection Profile, on the other hand, is a component that enables you to configure firewall resource protection settings for individual IP addresses or subnets. A QoS Profile is a component that enables you to configure quality of service settings for traffic passing through the firewall. A DoS Protection policy is a component that enables you to apply a DoS Protection Profile to specific traffic based on source and destination zones.

upvoted 2 times

[Removed] 11 months, 4 weeks ago

I think this one needs select 2

upvoted 1 times

PaloSteve 1 year, 1 month ago

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules>

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/dos-protection-profiles-and-policy-rules/dos-protection-profiles>

The question asks to "configure...protection settings"

DoS Protection policy rules determine the devices, users, zones, and services to which DoS Profiles apply.

DoS Protection profiles set thresholds that protect against new session IP flood attacks and provide resource protection (maximum concurrent session limits for specified endpoints and resources).

So I am leaning Answer A. The Profile gives the settings, and the policy describes what to protect.

upvoted 2 times

How can an administrator use the Panorama device-deployment option to update the apps and threat version of an HA pair of managed firewalls?

- A. Choose the download and install action for both members of the HA pair in the Schedule object
- B. Switch context to the firewalls to start the download and install process
- C. Download the apps to the primary no further action is required
- D. Configure the firewall's assigned template to download the content updates

Correct Answer: A

123XYZT 3 months ago

A, it's not D because they are only downloading and not installing.
upvoted 1 times

scanossa 7 months ago

Selected Answer: A

Device deployment is not related to any template
upvoted 1 times

confusion 1 year, 10 months ago

Selected Answer: A

A
Panorama > Device Deployment --> create Schedule, select "App and Threat", then select "Download And Install" and then select each member in the HA pair.
upvoted 1 times

TAKUM1y 1 year, 10 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-firewalls/use-case-configure-firewalls-using-panorama/set-up-your-centralized-configuration-and-policies/add-the-managed-firewalls-and-deploy-updates>
upvoted 2 times

datz 1 year, 11 months ago

Selected Answer: A

A

Select PanoramaDevice DeploymentDynamic Updates.
Click Check Now to check for the latest updates. If the value in the Action column is Download, this indicates an update is available.
Click Download. When the download completes, the value in the Action column changes to Install.
In the Action column, click Install. Use the filters or user-defined tags to select the managed firewalls on which you would like to install this update.
Click OK, then monitor the status, progress, and result of the content update for each firewall. The Result column displays the success or failure of the installation.
upvoted 1 times

Alen 1 year, 11 months ago

A. <https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/manage-firewalls/use-case-configure-firewalls-using-panorama/set-up-your-centralized-configuration-and-policies/add-the-managed-firewalls-and-deploy-updates>.
upvoted 1 times

secdaddy 1 year, 11 months ago

Looks like A to me :
<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/panorama-web-interface/panorama-device-deployment/schedule-dynamic-content-updates>
upvoted 2 times

millosz222 1 year, 11 months ago

Selected Answer: D

i think D
upvoted 1 times

A Panorama administrator configures a new zone and uses the zone in a new Security policy. After the administrator commits the configuration to Panorama, which device-group commit push operation should the administrator use to ensure that the push is successful?



- A. merge with candidate config
- B. include device and network templates
- C. specify the template as a reference template
- D. force template values

Correct Answer: A

  **ali_sh85** 1 month, 2 weeks ago



Selected Answer: B

B is correct not related to the candidate config
upvoted 1 times

  **Whizdhum** 8 months, 3 weeks ago


Selected Answer: B

Answer is B. To ensure that commit of template configurations work when referencing Device Group object, the commit must be done from the Device Group tab, with "Include Device and Network Templates" option enabled.
upvoted 1 times

  **Sammy3637** 8 months, 3 weeks ago

Selected Answer: B

After Panorama push ,next step is to push it to the devices
upvoted 1 times



  **certprep2021** 1 year, 6 months ago

Selected Answer: B



"Commit from Device Group, with the Include Network and Device Template option enabled to allow the template push to succeed along with the Device Group references."

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClpwCAC>

upvoted 3 times

  **VickiF** 1 year, 7 months ago

But, the question specifies device group push.
upvoted 1 times

  **Mmiri** 11 months, 1 week ago

[https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-commit-operations#:~:text=\(Selected%20by%20default\)%20Pushes%20both%20the%20device%20group%20changes%20and%20the%20associated%20template%20changes%20to%20the%20selected%20firewalls%20and%20virtual%20systems%20in%20a%20single%20operation.%20To%20push%20these%20changes%20as%20separate%20operations%2C%20clear%20this%20option.](https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-commit-operations#:~:text=(Selected%20by%20default)%20Pushes%20both%20the%20device%20group%20changes%20and%20the%20associated%20template%20changes%20to%20the%20selected%20firewalls%20and%20virtual%20systems%20in%20a%20single%20operation.%20To%20push%20these%20changes%20as%20separate%20operations%2C%20clear%20this%20option.)

upvoted 1 times

  **TAKUM1y** 1 year, 9 months ago

Selected Answer: B

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClpwCAC>

upvoted 2 times

  **confusion** 1 year, 10 months ago

Selected Answer: B

B
Template to get the Zone applied on the FW.
Device-group to get the Security Policy applied on the FW.
upvoted 1 times



  **Kuronekosama** 1 year, 11 months ago

B

A: cleared to ignore local candidate config
D: Will work, but you'll wipe out all the local config changes on that firewall. Not wrong, but not a great answer.
upvoted 1 times

  **secdaddy** 1 year, 11 months ago

A and B are both default
C isn't listed as a push operation
Why not D to 'ensure that the push is successful ?
<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-commit-operations>
upvoted 1 times

  **scally** 1 year, 11 months ago

Selected Answer: B

B is the correct answer. You need to push both the template and device group.
upvoted 3 times



Question #271

Topic 1

What would allow a network security administrator to authenticate and identify a user with a new BYOD-type device that is not joined to the corporate domain?

- A. a Security policy with 'known-user' selected in the Source User field
- B. a Security policy with 'unknown' selected in the Source User field
- C. an Authentication policy with 'known-user' selected in the Source User field
- D. an Authentication policy with 'unknown' selected in the Source User field



Correct Answer: D

  **blahblah1234567890000** 1 year, 4 months ago

Selected Answer: D

Whenever a user requests a resource, the firewall evaluates Authentication policy. Based on the matching policy rule, the firewall then prompts the user to respond to one or more challenges of different factors (types), such as login and password, voice, SMS, push, or one-time password (OTP) authentication. After the user responds to all the factors, the firewall evaluates Security policy (see Policies > Security) to determine whether to allow access to the resource.

upvoted 2 times

  **blahblah1234567890000** 1 year, 4 months ago

Select the source users or user groups to which the rule applies:

any—Includes any traffic regardless of source user.

pre-logout—Includes remote users who are not logged into their client systems but whose client systems connect to the network through the GlobalProtect pre-logout feature .

known-user—Includes all users for whom the firewall already has IP address-to-username mappings before the rule evokes authentication.

unknown—Includes all users for whom the firewall does not have IP address-to-username mappings. After the rule evokes authentication, the firewall creates user mappings for unknown users based on the usernames they entered.

Select—Includes only the users and user groups that you Add to the Source User list.

upvoted 3 times


  **confusion** 1 year, 10 months ago

Selected Answer: D

D

unknown—Includes all users for whom the firewall does not have IP address-to-username mappings. After the rule evokes authentication, the firewall creates user mappings for unknown users based on the usernames they entered.



upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/policies/policies-authentication/building-blocks-of-an-authentication-policy-rule>

upvoted 2 times

  **bimyo** 1 year, 11 months ago

Seems D is correct, as authentication policy with with the "Unknown", as

unknown—Includes all users for whom the firewall does not have IP address-to-username mappings. After the rule evokes authentication, the firewall creates user mappings for unknown users based on the usernames they entered.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/policies/policies-authentication/building-blocks-of-an-authentication-policy-rule>

upvoted 3 times

An administrator needs firewall access on a trusted interface. Which two components are required to configure certificate-based, secure authentication to the web UI? (Choose two.)

- A. server certificate
- B. SSL/TLS Service Profile
- C. certificate profile
- D. SSH Service Profile

Correct Answer: BC

Od2fdfa 3 months, 2 weeks ago

Selected Answer: AC

Correct option is A and C
There is no such thing called certificate profile under SSL/TLS service Profile.
Server certificate in this context is the local certificate on the firewall.
upvoted 2 times

Bubu3k 6 months ago

Selected Answer: AC

There is no mention of SSL profile:
<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-administrative-accounts-and-authentication/configure-certificate-based-administrator-authentication-to-the-web-interface>
upvoted 1 times

Pacheco 6 months, 3 weeks ago

Selected Answer: BC

I see a lot of people voting for A and there's no such thing as a "server certificate" needed for auth <<<to>>> the firewall, but you do need B and C to secure access <<<to>>> it. You can always work with the default server (fw) cert, so a server cert isn't really needed.

The server cert could be used inside the ssl/tls profile to define the cert <<<the fw will show to end devices>>>, but if you're authenticating <<<to the fw>>> you need the ssl/tls profile to define things like min and max tls versions and protocols supported <<<to access the web interface (that is acting as a web server)>>>

The cert profile specifies the CA that signs the client (end device)'s cert and other things like blocking options and CRL/OCSP settings, and has to be attached to a user account for cert-based auth.
upvoted 3 times

SH_ 7 months ago

Selected Answer: BC

B for secure authentication to webUI, and C for certificate-based authentication.
upvoted 4 times

tertiusgouws 7 months, 2 weeks ago

This question doesn't seem to be worded correctly. It's asking about authentication, not access. For authentication you need a Certificate Profile and a CA certificate, not a server certificate. When a username is entered that requires Certificate-based authentication, the firewall checks whether the certificate presented by the client is signed by the CA configured in the Certificate Profile. Nowhere in the authentication process is the firewall's own server certificate involved. So either the question is worded incorrectly and it should read "... secure *access* to the web UI?" instead of "... secure *authentication* to the web UI?" or A should be CA certificate instead of server certificate.
upvoted 1 times

JRKhan 7 months, 3 weeks ago

Selected Answer: AB

See question 261. Server certificates are most likely to be used with SSL/TLS profile. The question doesn't mention client authentication using certificates (so C is not valid and if you do select C then the best practice is to use a CA certificate not a server certificate); also it doesn't say mutual authentication so BC doesn't fit either. So I believe AB are the correct options as the minimum you can do is for the firewall to provide a server cert to the client to prove its identity.
upvoted 2 times

Whizdhum 8 months, 3 weeks ago

Selected Answer: AB

Answers are A, B. SSL/TLS service profiles specify a server certificate and a protocol version or range of versions for firewall or Panorama services that use SSL/TLS (such as administrative access to the web interface). Do not use certificate authority (CA) certificates for SSL/TLS services; use only signed certificates.
upvoted 3 times

[-]  **Pnosuke** 9 months, 3 weeks ago

CA and Cert Profile must be on the FW. Not the server cert. So, C is the only valid answer.


upvoted 3 times

[-]  **Omid2022** 10 months, 1 week ago

Selected Answer: AB

For WEB UI Management secure access on the Firewall, you only need A and B. If you want to config WEB UI secure access with a valid certificate you can import the cert via A and then create a SSL/TLS Service Profile. Finally you must use the TLS profile (B) under Device>Setup>General Settings>Click on Gear and the under SSL/TLS Service Profile select the generated TLS Service Profile :)

upvoted 3 times

[-]  **dgonz** 11 months, 2 weeks ago

Selected Answer: AC

certification profile defines user and device authentication for web interface access to Palo Alto Networks firewalls or Panorama you need a server certificate to set this up

upvoted 1 times

[-]  **Pochex** 1 year, 2 months ago

C is the only valid answer, A and B are used for the client to authenticate the firewall (server), and D will not use certs at all.

upvoted 1 times


[-]  **[Removed]** 1 year, 4 months ago

A and B!!!!!!!

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIFGCA0>

you need a ssl tls service profile (where you have to select the SERVER certificate that firewall will use to have https running without problems, In other words, the cert that is going to present to the WEB UI users)

upvoted 3 times

[-]  **laroux** 1 year, 3 months ago

This doesn't seem to be for authentication, just to use a specific certificate for the WEB UI.

upvoted 1 times

[-]  **Vahid4900** 1 year, 5 months ago

Selected Answer: AC

A and C- Certificate profile is use for verifying client certificates

upvoted 1 times

[-]  **Sarbi** 1 year, 8 months ago

100 % sure A and C. Did many times.

upvoted 2 times

[-]  **mz101** 1 year, 9 months ago

Should be AC.

Both SSH and SSL/TLS profiles are not necessary for certificate based admin authentication, based on the doc from the web link.

upvoted 3 times

[-]  **TAKUM1y** 1 year, 9 months ago

Selected Answer: AC

not answer is B

upvoted 2 times

[-]  **Flipower** 1 year, 9 months ago

A- <https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-administrative-accounts-and-authentication/configure-certificate-based-administrator-authentication-to-the-web-interface>


And C

upvoted 1 times

An administrator is building Security rules within a device group to block traffic to and from malicious locations. How should those rules be configured to ensure that they are evaluated with a high priority?


- A. Create the appropriate rules with a Block action and apply them at the top of the local firewall Security rules
- B. Create the appropriate rules with a Block action and apply them at the top of the Security Pre-Rules
- C. Create the appropriate rules with a Block action and apply them at the top of the Security Post-Rules
- D. Create the appropriate rules with a Block action and apply them at the top of the Default Rules

Correct Answer: B

  **Sammy3637** 8 months, 3 weeks ago

Selected Answer: B

Pre Rules come first always !
upvoted 1 times

  **confusion** 1 year, 10 months ago

Selected Answer: B

B, rule evaluation order is: Pre/Local/Post/Default
upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/defining-policies-on-panorama>
upvoted 2 times


  **mysteryzjoker** 1 year, 10 months ago

B - pre rules are evaluated first, then local, then post and the default rules are at the bottom
upvoted 2 times

When planning to configure SSL Forward Proxy on a PA-5260, a user asks how SSL decryption can be implemented using a phased approach in alignment with Palo Alto Networks best practices. What should you recommend?

- A. Enable SSL decryption for known malicious source IP addresses
- B. Enable SSL decryption for malicious source users
- C. Enable SSL decryption for source users and known malicious URL categories
- D. Enable SSL decryption for known malicious destination IP addresses

Correct Answer: C

  **secdaddy** Highly Voted 1 year, 11 months ago

Agree C

"Phase in decryption. Plan to decrypt the riskiest traffic first (URL Categories most likely to harbor malicious traffic, such as gaming or high-risk) and then decrypt more as you gain experience."

<https://docs.paloaltonetworks.com/best-practices/9-1/decryption-best-practices/decryption-best-practices/plan-ssl-decryption-best-practice-deployment>

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIEZCA0>



upvoted 5 times

  **Sammy3637** Most Recent 8 months, 3 weeks ago

Selected Answer: C

The options are a bit confusing but daddy of security explains it well in the comments

upvoted 1 times

  **lol12** 1 year, 8 months ago

Selected Answer: C

C

Basically choose control group of users and decrypt to known malicious URI's

upvoted 1 times

  **confusion** 1 year, 10 months ago

Selected Answer: C

C

phased starting with specific URL categories



upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/best-practices/10-2/decryption-best-practices/decryption-best-practices/plan-ssl-decryption-best-practice-deployment>

upvoted 2 times

  **bimyo** 1 year, 11 months ago

C - seems to be correct as the phased approach talks about URL categories. (Financial services & Health-and-medicine) are often times not allowed by law to decrypt. Also it talks about minimizing the impact for end-users. So enabling rule for some user groups and only for specific and malicious URL categories seems to be by far the most correct choice here.

upvoted 4 times

What are two valid deployment options for Decryption Broker? (Choose two.)

- A. Transparent Bridge Security Chain
- B. Transparent Mirror Security Chain
- C. Layer 2 Security Chain
- D. Layer 3 Security Chain

Correct Answer: AD

👤 **thelittleyellowbirdie** 3 weeks, 1 day ago

Two types of security chain deployments are supported: Layer 3 security chains and Transparent Bridge security chains.
upvoted 1 times

👤 **confusion** 1 year, 10 months ago

Selected Answer: AD

AD
<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-broker>
upvoted 1 times

👤 **TAKUM1y** 1 year, 10 months ago

Selected Answer: AD

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/decryption-broker/decryption-broker-concepts>
upvoted 3 times

👤 **mizuno92** 1 year, 11 months ago

Selected Answer: AD

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/decryption-broker/decryption-broker-concepts>
upvoted 2 times

👤 **mysteryjoker** 1 year, 11 months ago

AD is correct :
<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-broker>
upvoted 2 times

A network security engineer is attempting to peer a virtual router on a PAN-OS firewall with an external router using the BGP protocol. The peer relationship is not establishing. What command could the engineer run to see the current state of the BGP state between the two devices?

- A. show routing protocol bgp rib-out
- B. show routing protocol bgp peer
- C. show routing protocol bgp summary
- D. show routing protocol bgp state

Correct Answer: B

  **Sammy3637** 8 months, 3 weeks ago

Selected Answer: B

"attempting to peer"
upvoted 1 times

  **BrockHarbor** 1 year, 1 month ago

It is between show peer and show summary.

Because show peer gives you more info about your peer config, which will need to be verified, B is the best answer. Show summary will give you less info about the peer config and more info about the peering session, which is not established anyways and is therefore less helpful.

upvoted 3 times

  **ConfuzedOne** 1 year, 3 months ago

This live community post has output from both "show peer" and "show summary"
<https://live.paloaltonetworks.com/t5/general-topics/bgp-quot-router-id-quot-and-multiple-peers/td-p/24305>
- BOTH show the status / current state between the two devices.

Show Peer:
Peer status: Established, for 3657 seconds

Show summary:
peer peer1.4.1: AS 65002, Established, IP 10.10.10.4
upvoted 1 times

  **confusion** 1 year, 10 months ago

Selected Answer: B

Difficult to chose as both provide the BGP peer state:

- B. show routing protocol bgp peer
- C. show routing protocol bgp summary


Probably B is a little bit more correct answer as the output is split by peers with additional details and there is also an option to add "peer-name <name>" which will filter output for only specific peer, summary shows them all.

upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: B

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000CpwaCAC&lang=en_US%E2%80%A9
upvoted 3 times

  **fireb** 1 year, 10 months ago

Option B is correct.

<https://live.paloaltonetworks.com/t5/general-topics/monitoring-bgp-stats-from-palo-alto-panorama/td-p/24689>
upvoted 2 times

  **mysteryzjoker** 1 year, 10 months ago

not sure here would be good to know. All the commands bar D) are valid syntax
upvoted 2 times



What is the best description of the HA4 Keep-alive Threshold (ms)?

- A. the timeframe that the local firewall waits before going to Active state when another cluster member is preventing the cluster from fully synchronizing
- B. the timeframe within which the firewall must receive keepalives from a cluster member to know that the cluster member is functional
- C. the maximum interval between hello packets that are sent to verify that the HA functionality on the other firewall is operational
- D. the time that a passive or active-secondary firewall will wait before taking over as the active or active-primary firewall

Correct Answer: B

  **PaloSteve** 1 year, 1 month ago

This is VERY close to a PCNSE practice question. The answer there for the HA4 timer is:
The maximum interval between hello packets that are sent to verify that the HA functionality on the other firewall is operational.
From the HA links section of the PCNSE Study Guide:
HA cluster members use an HA4 link and HA4 backup link to perform session state synchronization.
HA1 (control link), HA2 (data link), and HA3 (packet-forwarding link) are not supported between cluster members that aren't HA pairs.
upvoted 1 times

  **confusion** 1 year, 10 months ago

Selected Answer: B

B
(Optional) Change the HA4 Keep-alive Threshold (ms) to specify the timeframe within which the firewall must receive keepalives from a cluster member to know that the cluster member is functional; range is 5,000 to 60,000; default is 10,000.
upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/configure-ha-clustering>
upvoted 2 times

  **west33637** 1 year, 10 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/high-availability/configure-ha-clustering>
STEP 3
upvoted 3 times

An engineer is tasked with enabling SSL decryption across the environment. What are three valid parameters of an SSL Decryption policy? (Choose three.)



- A. GlobalProtect HIP
- B. source users
- C. App-ID
- D. URL categories
- E. source and destination IP addresses

Correct Answer: ACE

  **nose999** Highly Voted 1 year, 12 months ago

Selected Answer: BDE

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/define-traffic-to-decrypt/create-a-decryption-policy-rule>
upvoted 7 times



  **bimyo** 1 year, 11 months ago

BDE is correct, checked it in LAB
upvoted 3 times

  **ali_sh85** Most Recent 1 month, 2 weeks ago

Selected Answer: BDE

Decryption and Authentication policies dont use application
upvoted 1 times

  **327c7c8** 5 months ago

Selected Answer: BDE

You cannot decrypt any traffic from any type of VPN, if it is GlobalProtect or AnyConnect etc.
App-ID is a function in the NGFW not an element in which you can use in a oolicy.
But source user, Source IP and Destination IP you can use in the SSL decrypt policy.
there are HIP option you can use but this is not associated with the GlobalProtect.
upvoted 1 times

  **findkeywordcommand** 5 months, 2 weeks ago

Who decides about what is right here? You can easily check that App-ID or GlobalProtect HIP aren't in the Decryption Policy Rule options.
Disappointed with this site
upvoted 1 times

  **Erle1988** 1 year, 3 months ago

Selected Answer: BDE

BDE is correct
upvoted 1 times

  **[Removed]** 1 year, 4 months ago

BDE Buuuuut!!! im checking my firewall and you can put HIP at source tab.... so global protect hip should be ok i think :O
upvoted 1 times

  **certprep2021** 1 year, 6 months ago

Selected Answer: BDE

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIEZCA0>

"In particular, decryption can be based upon URL categories, source users, and source/destination IP addresses."
upvoted 3 times

  **djedeen** 1 year, 7 months ago

Selected Answer: BDE

BDE: <https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/decryption/define-traffic-to-decrypt/create-a-decryption-policy-rule>
upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

BDE.
1.Users—Select Source and set the Source User for whom to decrypt traffic.
2. IP addresses, address objects, and/or address groups—Select Source and/or Destination to match to traffic based on Source Address and/or the

Destination Address

3. Select Service/URL Category to set the rule to match to traffic based on service

upvoted 1 times

  **confusion** 1 year, 10 months ago

Selected Answer: BDE


BDE

Src: Zone, Address, User

Dst: Zone, Address

Service/URL category



upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: BDE

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/define-traffic-to-decrypt/create-a-decryption-policy-rule>

upvoted 2 times

  **Alen** 1 year, 11 months ago

Selected Answer: BDE

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/define-traffic-to-decrypt/create-a-decryption-policy-rule>

upvoted 3 times

An engineer is configuring Packet Buffer Protection on ingress zones to protect from single-session DoS attacks. Which sessions does Packet Buffer Protection apply to?



- A. It applies to existing sessions and is not global
- B. It applies to existing sessions and is global
- C. It applies to new sessions and is global
- D. It applies to new sessions and is not global

Correct Answer: B

  **hcir** 2 months ago

Indeed, the doc says "existing sessions and global", but in reality, PBP applies to existing and new sessions. PBP measures Connections per seconds and can drop packets of new sessions or discard existing sessions should they consume too many buffers. Basically, the doc is wrong, but for the PCNSE, we should of course answer "While zone and DoS protection apply to new sessions (connections) and are granular, Packet Buffer Protection applies to existing sessions and is global." If only globally applied, PBP drops packets using RED. When applied in a zone, it can also block (with the "block countdown threshold") for an amount of time

upvoted 2 times

  **JRKhan** 7 months, 3 weeks ago

Selected Answer: B

PBP applies to existing sessions. It is enabled globally and if enabled globally can also be applied to zones.

upvoted 1 times


  **hifumi_daisuki** 8 months, 2 weeks ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/packet-buffer-protection>
Yes, Buffer Protection can apply on each zone. But from doc it said "You must enable Packet Buffer Protection globally in order for it to be active in zones."

So there must be a global rule already being made. Thus I chose B.


upvoted 1 times

  **Whizdhum** 8 months, 3 weeks ago

Selected Answer: B

Answer is B. Although you don't configure Packet Buffer Protection in a Zone Protection profile or in a DoS Protection profile or policy rule, Packet Buffer Protection defends ingress zones. While zone and DoS protection apply to new sessions (connections) and are granular, Packet Buffer Protection applies to existing sessions and is global.

upvoted 1 times

  **RoamingFo** 9 months, 2 weeks ago

Selected Answer: A

It Applied on existing sessions.

It is not Global, yes there is a global control but there is also a zone control, so it can be disabled on some zone.

Correct Answer is A

upvoted 1 times

  **Mocix** 10 months ago

What about "on ingress zones" part of the question? shouldn't the answer be A?

upvoted 1 times

  **confusion** 1 year, 10 months ago

Selected Answer: B

B

Global and applies to existing sessions.

upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/packet-buffer-protection>

upvoted 4 times

  **datz** 1 year, 11 months ago

Selected Answer: B

Packet Buffer Protection applies to existing sessions and is global.

Correct

upvoted 2 times

  **kulpaddy** 1 year, 11 months ago

Selected Answer: B

B correct answer. <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense/packet-buffer-protection>

upvoted 3 times

What are two best practices for incorporating new and modified App-IDs? (Choose two.)

- A. Run the latest PAN-OS version in a supported release tree to have the best performance for the new App-IDs
- B. Study the release notes and install new App-IDs if they are determined to have low impact
- C. Configure a security policy rule to allow new App-IDs that might have network-wide impact
- D. Perform a Best Practice Assessment to evaluate the impact of the new or modified App-IDs

Correct Answer: BC


  **ali_sh85** 1 month, 2 weeks ago

Selected Answer: AB

how C can be a correct answer?

Automatically allowing new App-IDs without careful assessment can introduce security risks. It is important to review and test new App-IDs before allowing them in a production environment.


upvoted 2 times

  **Whizdhum** 8 months, 3 weeks ago

Selected Answer: BC

Answers are B, C. Always review Content Release Notes for the list of newly-identified and modified application and threat signatures that the content release introduces. Configure a security policy rule to always allow new App-IDs that might have network-wide impact, like authentication or software development applications.

upvoted 1 times

  **Sammy3637** 8 months, 3 weeks ago

Selected Answer: BC

You can also review Content Release Notes for apps and threats on the Palo Alto Networks Support Portal or directly in the firewall web interface:



select Device

Dynamic Updates

and open the Release Note

for a specific content release version.

upvoted 1 times

  **Billyon** 10 months, 2 weeks ago

Selected Answer: BD

upvoted 1 times

  **TAKUM1y** 1 year, 9 months ago

Selected Answer: BC

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/software-and-content-updates/best-practices-for-app-and-threat-content-updates/best-practices-security-first#id184AH00F06E>

upvoted 2 times

  **confusion** 1 year, 10 months ago

Selected Answer: BC

BC

Release notes + Security Policy

upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: BC

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-releases/app-id-updates-workflow>

upvoted 1 times

  **mysteryzjoker** 1 year, 11 months ago

BC

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-releases/app-id-updates-workflow#id182P00F0FEI>

upvoted 2 times

The manager of the network security team has asked you to help configure the company's Security Profiles according to Palo Alto Networks best practice. As part of that effort, the manager has assigned you the Vulnerability Protection profile for the Internet gateway firewall. Which action and packet-capture setting for items of high severity and critical severity best matches Palo Alto Networks best practice?

- A. action 'reset-server' and packet capture 'disable'
- B. action 'default' and packet capture 'single-packet'
- C. action 'reset-both' and packet capture 'extended-capture'
- D. action 'reset-both' and packet capture 'single-packet'

Correct Answer: D

mysteryzjoker Highly Voted 1 year, 11 months ago

answer is C

"Enable extended-capture for critical, high, and medium severity events and single-packet capture for low severity events. "

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-security-profiles-vulnerability-protection>

upvoted 22 times

secdaddy 1 year, 10 months ago

See the best practices document (kudos to GBD35055 for the URL) :

The best practice Anti-Spyware profile retains the default Action to reset the connection when the firewall detects a medium, high, or critical severity threat, and enables single packet capture (PCAP) for those threats.

<https://docs.paloaltonetworks.com/best-practices/10-2/data-center-best-practices/data-center-best-practice-security-policy/how-to-create-data-center-best-practice-security-profiles/create-the-data-center-best-practice-anti-spyware-profile>

upvoted 3 times

fireb 1 year, 10 months ago

Option C is correct.

upvoted 2 times

confusion 1 year, 10 months ago

No, D is correct! Question asks for Best Practice Internet Gateway Vulnerability Protection Profile.

upvoted 3 times

droide 1 year, 6 months ago

Still the same in pan-os 11.0

upvoted 2 times

Od2fdfa Most Recent 3 months, 2 weeks ago

Selected Answer: D

Option D is correct

Option C is wrong

This is internet Gateway Firewall. Packet captures on Internet gateway firewall does not make sense. Firewall would rather shut the session.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIXCCA0>

Notice that Anti-Spyware and Vulnerability Protection have more options

Disabled

Single Packet

Select single-packet to capture one packet when a threat is detected.

Extended-capture

Select the extended-capture option to capture more packets. Extended-capture will provides much more context to the threat when analyzing the threat logs or when providing the captures for TAC to analyze.

upvoted 1 times

MostafaNawar 4 months, 4 weeks ago

Selected Answer: C

Answer C, Enable extended-capture for critical, high, and medium severity events and single-packet capture for low severity events. Use the default extended-capture value of 5 packets, which provides enough information to analyze the threat in most cases.


upvoted 2 times

Thunnu 5 months, 4 weeks ago

Yup D.

<https://docs.paloaltonetworks.com/best-practices/9-1/internet-gateway-best-practices/best-practice-internet-gateway-security-policy/create-best-practice-security-profiles>


upvoted 2 times

[-]  **JRKhan** 7 months, 3 weeks ago

Selected Answer: D

Correct answer is D. For inbound traffic aka internet traffic to the network behind paloalto firewall, the best practice is to use strict profile which uses *reset-both* action for critical/high sev events. For pcaps, use *single pcap* as the traffic volume is usually high. Can also use extended captures if the action is set to *alert*.


upvoted 1 times

[-]  **Whizdhum** 8 months, 3 weeks ago

Selected Answer: D


Clone the predefined strict Vulnerability Protection profile and edit it to create the best practice profile: Change the Action in the three brute force rules to reset-both and Packet Capture to single-packet to transition from alerting on brute-force attack events to blocking them. Consolidate critical, high, and medium severity events for servers and clients into one rule. Set the Action to reset-both and set Packet Capture to single-packet. This simplifies the profile and works because the profile uses the same action and the same packet capture settings for these severities.

upvoted 1 times

[-]  **Metgatz** 8 months, 4 weeks ago

C is the correct option: action 'reset-both' and packet capture 'extended-capture'

upvoted 2 times

[-]  **RoamingFo** 9 months, 2 weeks ago

Selected Answer: D

Recommended Action "Reset-Both"


Recommended Capture ?

This General doc recommends "Enable extended-capture for critical, high, and medium severity" <https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-web-interface-help/objects/objects-security-profiles-vulnerability-protection>

The Internet Gateway Specific Doc Recommends "Consolidate critical, high,... Set the Action to reset-both and set Packet Capture to single-packet"

Correct Answer is D

upvoted 2 times

[-]  **dorf05** 10 months, 3 weeks ago

Selected Answer: D

<https://docs.paloaltonetworks.com/best-practices/internet-gateway-best-practices/best-practice-internet-gateway-security-policy/create-best-practice-security-profiles#:~:text=end%20user%E2%80%99s%20device.-,Best%20Practice%20Internet%20Gateway%20Vulnerability%20Protection%20Profile,same%20action%20and%20the%20same%20packet%20capture%20settings%20for%20these%20severities.,-For%20profiles%20that>

upvoted 1 times

[-]  **Betty2022** 1 year ago

Selected Answer: D

D is correct Question asks for Best Practice Internet Gateway Vulnerability Protection Profile.

<https://docs.paloaltonetworks.com/best-practices/internet-gateway-best-practices/best-practice-internet-gateway-security-policy/create-best-practice-security-profiles>

Change the Action in the three brute force rules to reset-both and Packet Capture to single-packet to transition from alerting on brute-force attack events to blocking them.


Consolidate critical, high, and medium severity events for servers and clients into one rule. Set the Action to reset-both and set Packet Capture to single-packet. This simplifies the profile and works because the profile uses the same action and the same packet capture settings for these severities.

upvoted 3 times

[-]  **Pochex** 1 year, 3 months ago

Answer D is correct. Refer to <https://docs.paloaltonetworks.com/best-practices/10-2/internet-gateway-best-practices/best-practice-internet-gateway-security-policy/create-best-practice-security-profiles> and read the following section: 'Best Practice Internet Gateway Vulnerability Protection Profile'

upvoted 1 times

[-]  **sujss** 1 year, 4 months ago

Selected Answer: D

"For the best practice profile, for each rule except simple-client-informational and simple-server-informational, double-click the Rule Name and change Packet Capture from disable to single-packet to enable packet capture (PCAP) for each rule so you can track down the source of potential attacks."

<https://docs.paloaltonetworks.com/best-practices/10-2/data-center-best-practices/data-center-best-practice-security-policy/how-to-create-data-center-best-practice-security-profiles/create-the-data-center-best-practice-vulnerability-protection-profile>

upvoted 1 times

[-]  **[Removed]** 1 year, 5 months ago

Selected Answer: C

For the best security, set the Action for both client and server critical, high, and medium severity events to reset-both and use the default action for Informational and Low severity events.

upvoted 1 times

[-]  **IntheZone** 1 year, 5 months ago

Selected Answer: C

"items of high severity and critical severity best matches Palo Alto Networks best practice"

It is C

upvoted 1 times

  **daytonadave2011** 1 year, 5 months ago

Selected Answer: D

D. Just went through some BPA's and single-capture is the recommended.

upvoted 1 times

  **Rowdy_47** 1 year, 6 months ago

Selected Answer: D

For the best practice profile, for each rule except simple-client-informational and simple-server-informational, double-click the Rule Name and change Packet Capture from disable to single-packet to enable packet capture (PCAP) for each rule so you can track down the source of potential attacks. Don't change the rest of the settings.



Apply extended PCAP (as opposed to single PCAP) to high-value traffic to which you apply the alert Action

We would not be setting an alert action on high severity and critical severity matches

I think the answer is D

<https://docs.paloaltonetworks.com/best-practices/10-2/internet-gateway-best-practices/best-practice-internet-gateway-security-policy/create-best-practice-security-profiles>



upvoted 1 times

  **droide** 1 year, 6 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/objects/objects-security-profiles-vulnerability-protection>

upvoted 1 times

  **droide** 1 year, 6 months ago

Sorry, must be D according to Palo Alto Networks best practice

upvoted 1 times

Question #282

Topic 1

An engineer needs to redistribute User-ID mappings from multiple data centers. Which data flow best describes redistribution of user mappings?

- A. User-ID agent to firewall
- B. firewall to firewall
- C. Domain Controller to User-ID agent
- D. User-ID agent to Panorama

Correct Answer: B

  **confusion** 1 year, 10 months ago

Selected Answer: B

B

for sure

upvoted 3 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id/deploy-user-id-in-a-large-scale-network/redistribute-user-mappings-and-authentication-timestamps/firewall-deployment-for-user-id-redistribution#ide3661b46-4722-4936-bb9b-181679306809>

upvoted 2 times

  **mysteryjoker** 1 year, 10 months ago

B is correct. Have configured this before.

upvoted 2 times

An administrator is attempting to create policies for deployment of a device group and template stack. When creating the policies, the zone drop-down list does not include the required zone. What must the administrator do to correct this issue?

- A. Add a firewall to both the device group and the template
- B. Add the template as a reference template in the device group
- C. Enable "Share Unused Address and Service Objects with Devices" in Panorama settings
- D. Specify the target device as the master device in the device group

Correct Answer: A


  **scally** Highly Voted  1 year, 11 months ago

Selected Answer: B

In order to see what is in a template, the device-group needs the template referenced. Even if you add the firewall to both the template and device-group, the device-group will not see what is in the template. The following link has a video that demonstrates that B is the correct answer.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNfeCAG>

upvoted 27 times

  **nose999** 1 year, 11 months ago

Great find!

upvoted 1 times

  **0d2fdfa** Most Recent  3 months, 2 weeks ago

Selected Answer: B

Thanks Scally. The video explains everything.

A is wrong folks.



upvoted 1 times

  **scanossa** 6 months, 3 weeks ago

Selected Answer: B

B is the correct answer

upvoted 1 times

  **Sarbi** 1 year, 8 months ago

The correct answer is B

upvoted 1 times

  **confusion** 1 year, 10 months ago

Selected Answer: B



B, link from "scally" is very useful

upvoted 1 times

What best describes the HA Promotion Hold Time?



- A. the time that the passive firewall will wait before taking over as the active firewall after communications with the HA peer have been lost
- B. the time that is recommended to avoid a failover when both firewalls experience the same link/path monitor failure simultaneously
- C. the time that is recommended to avoid an HA failover due to the occasional flapping of neighboring devices
- D. the time that a passive firewall with a low device priority will wait before taking over as the active firewall if the firewall is operational again

Correct Answer: A

  **Sammy3637** 8 months, 3 weeks ago



Selected Answer: A

A is correct
upvoted 1 times

  **sujss** 1 year, 4 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/high-availability/ha-concepts/ha-timers>
upvoted 1 times


  **DenskyDen** 1 year, 7 months ago

A.
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clx4CAC#:~:text=The%20Promotion%20Hold%20Time%20is,5%20seconds>).
upvoted 1 times

  **confusion** 1 year, 10 months ago

Selected Answer: A

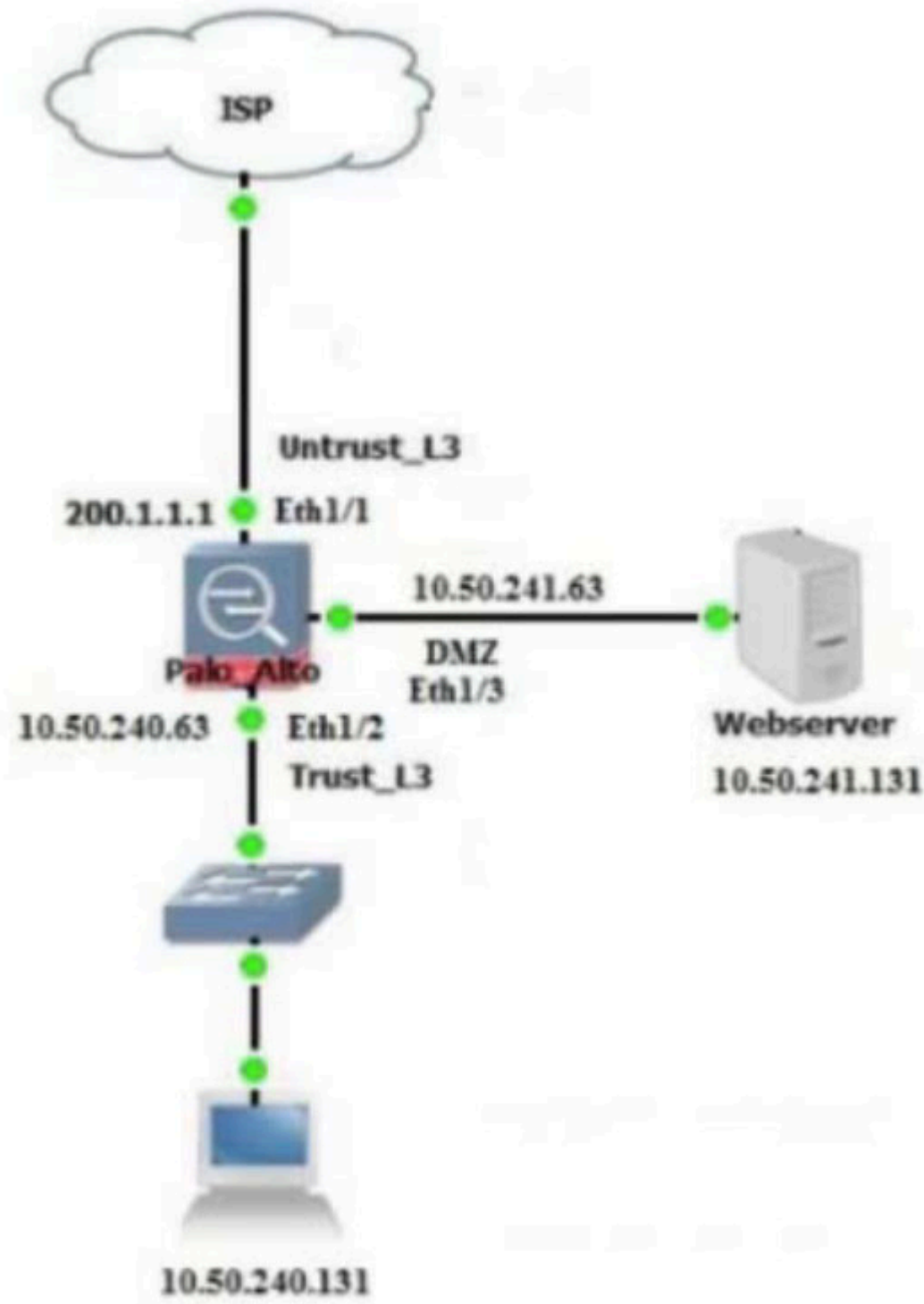
A, link from "fireb" is exact definition.
upvoted 2 times

  **fireb** 1 year, 10 months ago

Option A is correct.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clx4CAC>
upvoted 4 times

A user at an internal system queries the DNS server for their web server with a private IP of 10.250.241.131 in the DMZ. The DNS server returns an address of the web servers public address, 200.1.1.10. In order to reach the web server, which security rule and U-Turn NAT rule must be configured on the firewall?



- A. NAT Rule: Source Zone: Untrust_L3 Source IP: Any Destination Zone: DMZ Destination IP: 200.1.1.10 Destination Translation address: 10.250.241.131 Security Rule: Source IP: Any Destination Zone: DMZ Destination IP: 10.250.241.131
- B. NAT Rule: Source Zone: Trust_L3 Source IP: Any Destination Zone: DMZ Destination IP: 200.1.1.10 Destination Translation address: 10.250.241.131 Security Rule: Source Zone: Untrust-L3 Source IP: Any Destination Zone: DMZ Destination IP: 10.250.241.131
- C. NAT Rule: Source Zone: Untrust_L3 Source IP: Any Destination Zone: Untrust_L3 Destination IP: 200.1.1.10 Destination Translation address: 10.250.241.131 Security Rule: Source Zone: Untrust-L3 Source IP: Any Destination Zone: DMZ Destination IP: 10.250.241.131
- D. NAT Rule: Source Zone: Trust_L3 Source IP: Any Destination Zone: Untrust_L3 Destination IP: 200.1.1.10 Destination Translation address: 10.250.241.131 Security Rule: Source Zone: Trust-L3 Source IP: Any Destination Zone: DMZ Destination IP: 200.1.1.10

Correct Answer: D

sov4 1 year, 1 month ago

Selected Answer: D

Had this question on the exam a few weeks ago... July 2023.
upvoted 4 times



franko_72 8 months, 3 weeks ago

Yep so did I, similar time, June/July.
upvoted 1 times

Kalipso21 1 year, 7 months ago



Answer is D, this is explained in an scenario here <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIEiCAK>

upvoted 4 times

  **sujss** 1 year, 4 months ago



Thanks for this

upvoted 1 times

  **DenskyDen** 1 year, 7 months ago

D. Agree


upvoted 1 times

  **confusion** 1 year, 10 months ago

Selected Answer: D

Security rules use pre-NAT IP and post-NAT Zone

upvoted 2 times



  **mysteryzjoker** 1 year, 10 months ago

D)

Great PAN NAT video here, includes Uturn NAT

<https://www.youtube.com/watch?v=Ahrao6kBg8w&t=566s>

upvoted 1 times

  **bimyo** 1 year, 11 months ago

Selected Answer: D



Yes D is correct, think it over again if your result is different.

upvoted 2 times

What is considered the best practice with regards to zone protection?

- A. Use separate log-forwarding profiles to forward DoS and zone threshold event logs separately from other threat logs
- B. Review DoS threat activity (ACC > Block Activity) and look for patterns of abuse
- C. Set the Alarm Rate threshold for event-log messages to high severity or critical severity
- D. If the levels of zone and DoS protection consume too many firewall resources, disable zone protection

Correct Answer: D

  **Od2fdfa** 3 months, 2 weeks ago



Selected Answer: A

Correct option is A
the question is about best practice. I don't think disabling Zone Protection would be a best practice regardless of circumstances.
upvoted 1 times

  **34f7d3a** 8 months, 3 weeks ago



Selected Answer: A

Log Forwarding—For easier management, forward DoS logs separately from other Threat logs directly to administrators via email and to a log server. - <https://docs.paloaltonetworks.com/best-practices/dos-and-zone-protection-best-practices/dos-and-zone-protection-best-practices/deploy-dos-and-zone-protection-using-best-practices>
upvoted 1 times

  **Sammy3637** 8 months, 3 weeks ago

Selected Answer: A

lol the answer is D , that's a big no no
it's best practice to use separate log forwarding profiles for DoS and ZPP event logs
upvoted 1 times

  **Metgatz** 8 months, 4 weeks ago

Option A - "For easier management, use separate log forwarding profiles to forward DoS and zone threshold event logs separately from other Threat logs." Best Practices: <https://docs.paloaltonetworks.com/best-practices/dos-and-zone-protection-best-practices/dos-and-zone-protection-best-practices/follow-post-deployment-dos-and-zone-protection-best-practices>
upvoted 1 times

  **electro165** 1 year ago

Selected Answer: B



Reviewing DoS (Denial of Service) threat activity in the Block Activity section of the ACC (Application Command Center) and looking for patterns of abuse is an important step in ensuring effective zone protection. By monitoring and analyzing DoS threat activity, you can identify potential attacks and take appropriate actions to mitigate them.
upvoted 1 times

  **certprep2021** 1 year, 6 months ago

Selected Answer: A



<https://docs.paloaltonetworks.com/best-practices/dos-and-zone-protection-best-practices/dos-and-zone-protection-best-practices/follow-post-deployment-dos-and-zone-protection-best-practices>

"For easier management, use separate log forwarding profiles to forward DoS and zone threshold event logs separately from other Threat logs."
upvoted 3 times

  **David010989** 1 year, 8 months ago

is D because the kb says Log Forwarding—For easier management, forward DoS logs separately from other Threat logs directly to administrators via email and to a log server.

only for easier mgmt but the real thing here are the fw resources
upvoted 1 times

  **lol12** 1 year, 8 months ago

Selected Answer: A

A

Disabling zone protection because not enough resources is hardly best practices. Best practice would be to size the appliance accordingly in the first place and so make D obsolete. Then A is correct.

<https://docs.paloaltonetworks.com/best-practices/dos-and-zone-protection-best-practices/dos-and-zone-protection-best-practices/deploy-dos-and-zone-protection-using-best-practices>

upvoted 3 times

  **Goharam** 1 year, 9 months ago

Look this.

"Measure firewall performance to ensure it's within acceptable norms and so you understand the effect of zone and DoS protection on firewall resources.

If the levels of zone and DoS protection (combined with other resource-consuming features such as decryption) consume too many firewall resources, the best practice is to scale up the resources rather than to compromise security."

So, the answer is not D. It's A.

upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/best-practices/10-1/dos-and-zone-protection-best-practices/dos-and-zone-protection-best-practices/follow-post-deployment-dos-and-zone-protection-best-practices>

upvoted 1 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: D

<https://docs.paloaltonetworks.com/best-practices/10-1/dos-and-zone-protection-best-practices/dos-and-zone-protection-best-practices/deploy-dos-and-zone-protection-using-best-practices>


upvoted 1 times

  **mysteryzjoker** 1 year, 10 months ago

annoyingly both A & B are included in the link:



<https://docs.paloaltonetworks.com/best-practices/9-1/dos-and-zone-protection-best-practices/dos-and-zone-protection-best-practices/follow-post-deployment-dos-and-zone-protection-best-practices>

upvoted 1 times

  **Flipower** 1 year, 9 months ago

B is incorrect. The link says (ACC > Threat Activity), NOT (ACC > Block Activity) like stated in B.

upvoted 1 times

  **datz** 1 year, 11 months ago

Selected Answer: A

A is correct answer. (Log forwarding)

Palo will never tell you as Best practice to disable security....

upvoted 1 times


  **al12345** 1 year, 11 months ago

Selected Answer: A

<https://docs.paloaltonetworks.com/best-practices/10-1/dos-and-zone-protection-best-practices/dos-and-zone-protection-best-practices/deploy-dos-and-zone-protection-using-best-practices>

Log Forwarding—For easier management, forward DoS logs separately from other Threat logs directly to administrators via email and to a log server.


upvoted 3 times

  **nose999** 1 year, 12 months ago

Selected Answer: B

<https://docs.paloaltonetworks.com/best-practices/9-1/dos-and-zone-protection-best-practices/dos-and-zone-protection-best-practices/follow-post-deployment-dos-and-zone-protection-best-practices>

upvoted 1 times

  **al12345** 1 year, 11 months ago

Review DoS threat activity (ACC - Threat Activity) and look for patterns of abuse. ?


correct is A

upvoted 1 times

An administrator allocates bandwidth to a Prisma Access Remote Networks compute location with three remote networks. What is the minimum amount of bandwidth the administrator could configure at the compute location?

- A. 90Mbps
- B. 75Mbps
- C. 50Mbps
- D. 300Mbps

Correct Answer: C

  **Whizdhum** 8 months, 3 weeks ago

Selected Answer: C

Answer is C. 50 Mbps is the minimum aggregate bandwidth that can be configured per compute location.
upvoted 2 times

  **Metgatz** 8 months, 4 weeks ago

C: 50Mbps
upvoted 1 times

  **djedeen** 1 year, 7 months ago

Selected Answer: C

Specify a minimum bandwidth of 50 Mbps and a maximum bandwidth of the maximum remaining licensed bandwidth.
upvoted 2 times

  **confusion** 1 year, 10 months ago

Selected Answer: C

C
50Mbps is the min.
upvoted 2 times

  **TAKUM1y** 1 year, 10 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prisma-access-for-networks/configure-prisma-access-for-networks/configure-bandwidth-by-compute-location#id2a91f76f-db22-4c25-8c25-91db3701d860>
"To verify the bandwidth amount you entered, select the check mark next to the bandwidth amount; to cancel the amount, select x.
Specify a minimum bandwidth of 50 Mbps and a maximum bandwidth of the maximum remaining licensed bandwidth."
upvoted 3 times

  **mizuno92** 1 year, 11 months ago

Selected Answer: C

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prisma-access-for-networks/configure-prisma-access-for-networks/configure-bandwidth-by-compute-location#id2a91f76f-db22-4c25-8c25-91db3701d860>
upvoted 4 times

An engineer must configure the Decryption Broker feature. Which Decryption Broker security chain supports bi-directional traffic flow?

- A. Layer 2 security chain
- B. Layer 3 security chain
- C. Transparent Bridge security chain
- D. Transparent Proxy security chain

Correct Answer: B

archer3129871 3 months ago

Answer is B

=====

The Decryption Broker feature supports two types of security chain networks:
Layer 3 security chains and Transparent Bridge security chains.

You can configure the firewall to direct traffic through the security chain either unidirectionally or bidirectionally1.

**When it comes to bi-directional traffic flow, the Layer 3 security chain is the one you're looking for. Let me provide more details about how it works:

The firewall uses the Primary Interface dedicated to decryption forwarding to forward both inbound and outbound sessions to the first security chain device.

The last security chain device forwards both inbound and outbound sessions back to the firewall2.

upvoted 1 times

Whizdhum 8 months, 3 weeks ago

Answers are B, C. The bidirectional flow option is available for both security chain types. Your network topology determines whether to use unidirectional or bidirectional flows. The performance is approximately the same using either method.

upvoted 2 times

GohanF2 1 year, 6 months ago

nasty question. both B and C are valid

upvoted 1 times

mz101 1 year, 9 months ago

Other than B, looks like that C is correct as well based on following:

"Set the Flow Direction for decrypted traffic the firewall forwards: Unidirectional or Bidirectional."

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/decryption-broker/decryption-broker-configure-with-transparent-bridge>

upvoted 1 times

TAKUM1y 1 year, 9 months ago

Selected Answer: B

B !! :

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/decryption-broker/security-chain-layer-3-guidelines>

upvoted 2 times

Alen 1 year, 10 months ago

B and C are correct here as stated above. Also Decryption broker is now called Network packet broker

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-new-features/networking-features/network-packet-broker>

upvoted 3 times

mizuno92 1 year, 11 months ago

Layer 3 and Transparent Bridge support Bidirectional

upvoted 4 times

An administrator is using Panorama to manage multiple firewalls. After upgrading all devices to the latest PAN-OS software, the administrator enables log forwarding from the firewalls to Panorama. However, pre-existing logs from the firewalls are not appearing in Panorama. Which action should be taken to enable the firewalls to send their pre-existing logs to Panorama?

- A. Use the import option to pull logs.
- B. Use the scp logdb export command.
- C. Export the log database.
- D. Use the ACC to consolidate the logs.

Correct Answer: B

TAKUM1y Highly Voted 1 year, 9 months ago

Selected Answer: C

Not command "scp logdb export".
enable command is "scp export logdb <XXX>"
upvoted 6 times

Od2fdfa Most Recent 3 months, 2 weeks ago

Selected Answer: C

Not command "scp logdb export".
upvoted 1 times

1f2c588 3 months, 2 weeks ago

B is correct, use the scp export commande with the cli: scp export logdb to <username@host:path_to_destination_filename>
upvoted 1 times

Whizdhum 8 months, 3 weeks ago

Selected Answer: C

Answer is C. The answer is C assuming that choice B was meant to be incorrect. By entering "scp export logdb to ..." on the CLI, you are essentially exporting the log database.
upvoted 1 times

Metgatz 8 months, 4 weeks ago

Correcto C option: scp export logdb ==> Correct command
scp logdb export ==> Wrong command
upvoted 1 times

Nawda 11 months, 3 weeks ago

Selected Answer: C

Panorama doesn't support scp export..
"Because the file for the entire log database is too large for an export or import to be practical on the following models, they do not support the scp export logdb or scp import logdb commands:
Panorama virtual appliance running Panorama 6.0 or later releases.
Panorama M-Series appliances (all releases)."

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-cli-quick-start/use-the-cli/use-secure-copy-to-import-and-export-files/export-and-import-a-complete-log-database-logdb>

upvoted 1 times

Pochex 1 year, 5 months ago

Answer C is correct, logdb stands for log database, but the command syntax in answer B is wrong:

scp export logdb ==> is good
scp logdb export ==> is not an option from the CLI
upvoted 3 times

lol12 1 year, 8 months ago

Selected Answer: C

I think C is correct. Export log database includes all steps needed to export it, i.e. commands.
B command is incorrect syntax.

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-cli-quick-start/use-the-cli/use-secure-copy-to-import-and-export-files/export-and-import-a-complete-log-database-logdb>

upvoted 3 times